

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-341266

(43)Date of publication of application : 08.12.2000

(51)Int.Cl.

H04L 9/14
 G06F 12/00
 G06F 12/14
 G06F 15/00
 G09C 1/00
 G10L 19/02
 G10L 19/00
 G10L 11/00
 H04L 9/20
 H04N 7/167

(21)Application number : 11-152208

(71)Applicant : VICTOR CO OF JAPAN LTD

(22)Date of filing : 31.05.1999

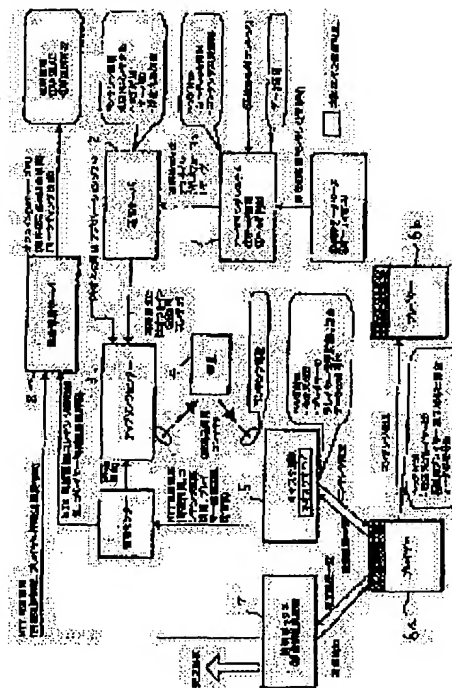
(72)Inventor : TANAKA YOSHIKI
 OKABE YASUHISA

(54) DATA TRANSFER METHOD, DATA TRANSFER METHOD IN CONTENTS SALES SYSTEM
 UTILIZING THE METHOD AND RECORDING MEDIUM RECORDING DATA

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent reproduction of real data from being hindered while preventing copying in a sales system for contents data such as music data.

SOLUTION: The contents sales system is a system where host serves contents data such as music and transfers (downloads) them to user side players 6a, 6b via a KIOSK installed terminal 5 and a network such as the Internet. A different encryption system is adopted for contents data requiring reproduction in an early timing from that for header information requiring no early timing, the encryption system not taking much time for decoding is adopted for the contents data and a complicated encryption system taking much time for decoding is adopted for the header information storing reproduction key information or the like.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-341266

(P2000-341266A)

(43)公開日 平成12年12月8日(2000.12.8)

(51)Int.Cl. ⁷	識別記号	F I	テラワード(参考)
H 0 4 L 9/14		H 0 4 L 9/00	6 4 1 5 B 0 1 7
G 0 6 F 12/00	5 4 5	G 0 6 F 12/00	5 4 5 M 5 B 0 8 2
	12/14		3 2 0 B 5 B 0 8 5
	15/00		3 3 0 Z 5 C 0 6 4
G 0 9 C 1/00	6 1 0	G 0 9 C 1/00	6 1 0 B 5 D 0 4 5

審査請求 未請求 請求項の数 3 O L (全 30 頁) 最終頁に続く

(21)出願番号 特願平11-152208

(22)出願日 平成11年5月31日(1999.5.31)

(71)出願人 000004329

日本ビクター株式会社

神奈川県横浜市神奈川区守屋町3丁目12番地

(72)発明者 田中 美昭

神奈川県横浜市神奈川区守屋町3丁目12番
地 日本ビクター株式会社内

(72)發明者 岡部 恭尚

神奈川県横浜市神奈川区守屋町3丁目12番
地 日本ビクター株式会社内

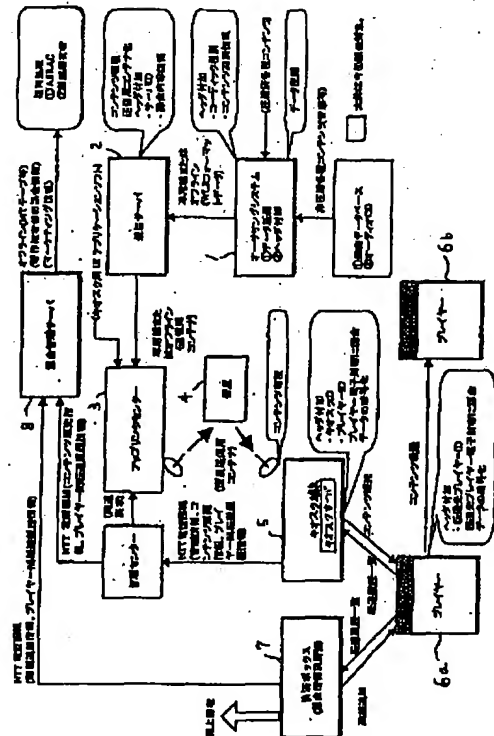
最終頁に続く

(54) 【発明の名称】 データの転送方法、その方法を利用したコンテンツ販売システムのデータ転送方法及びそのデータが記録された記録媒体

(57) 【要約】

【課題】 音楽データのようなコンテンツデータの販売システムにおいて、コピー防止を図りつつ、実データの再生に支障をきたすようなことがないようにする。

【解決手段】 音楽などのコンテンツデータをホストが提供してキオスク置端末5やインターネットなどのネットワークを介してユーザ側のプレーヤ6a, 6bに対して転送（ダウンロード）するコンテンツ販売システムであり、早いタイミングでの再生が要求されるコンテンツデータと、そこまでの要求がないヘッダ情報との暗号化方式を異ならせ、コンテンツデータの方を復号化に時間を要しない暗号化方式にし、再生鍵情報等が格納されるヘッダ情報の方を復号化に時間を要する複雑な暗号化方式にする。



【特許請求の範囲】

【請求項1】 転送元端末から転送先端末に対して、そのデータ再生時の処理速度が所定の速度で要求される第1のデータと、それより遅い処理速度の再生が許される第2のデータとを含んで転送するデータの転送方法において、

前記第1のデータを所定の第1の再生鍵を用いて暗号化すると共に、前記第2のデータを前記第1の再生鍵を用いて暗号化して復号化するときの処理速度より復号化に時間を要する第2の再生鍵を用いて暗号化し、これら暗号化された第1と第2のデータを転送するようにしたことを特徴とするデータの転送方法。

【請求項2】 前記データの転送方法は、販売元端末より販売先端末にコンテンツデータを配信するコンテンツ販売システムのデータ転送方法であり、

前記第1のデータは、少なくとも実データであるコンテンツデータであり、前記第2のデータは少なくとも前記コンテンツデータに付加されるヘッダ情報であり、前記第1の再生鍵による暗号化は、所定バイト数の乱数で生成された前記第1の再生鍵と前記コンテンツデータとをXOR演算により暗号化し、前記第2の再生鍵による暗号化は、所定バイトの乱数で生成された第2の再生鍵により前記第2のデータがDES暗号化されたものであることを特徴とするコンテンツ販売システムのデータ転送方法。

【請求項3】 請求項1又は2記載の転送方法により転送されたデータを所定の領域に記録したことを特徴とする記録媒体。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、音楽などのコンテンツデータをホストが提供して販売店設置端末やインターネットなどのネットワークを介してユーザ側のプレーヤに対して転送（ダウンロード）するデータの転送方法、その方法を利用したコンテンツ販売システムのデータ転送方法及びそのデータが記録された記録媒体に関する。

【0002】

【従来の技術】 近年、音楽などのコンテンツデータ（ソフト）をユーザ側に販売するシステムとして、CD（コンパクト・ディスク）やDVD（デジタル・バーサタイル・ディスク）などの有料の記録媒体を用いる代わりに、対価の支払いを条件として販売店設置端末やインターネットなどのネットワークを介してユーザ側のプレーヤ内のハードディスクや半導体メモリなどの記録媒体に転送してこれを再生するコンテンツ販売システムあるいはネットワーク配信システムが着目されている。

【0003】 コンテンツ販売システムの一例としては、コンテンツデータをホスト側から衛星通信回線や公衆電話回線を介して販売店設置端末に転送し、更に販売店設

置端末からプレーヤに転送する販売店設置端末経由方式が考えられる。他の経由方式としては、コンテンツデータをインターネット・サーバ（ホスト）側からインターネット及びインターネットクライアント（ユーザパソコン）を介してプレーヤに転送するインターネット経由方式が考えられる。

【0004】

【発明が解決しようとする課題】 ところで、このようなコンテンツ販売システムでは、不正にコンテンツデータがコピーされないように送信側のID（識別情報）や受信側のIDに基づいて暗号化してから送信するようなことが考えられている。ところが、そのように暗号化しても、何らかの手法によりIDが知られ、そのIDを用いて暗号を解読して不正なコピーが行われることが懸念されている。そこで、本発明では、このような問題に鑑みて不正なコピーが行われないような暗号化を行うと共に、より速い再生速度での再生が要求される例えば実データであるコンテンツデータと、それほど速い処理速度での再生が要求されない例えばヘッダ情報等との暗号化方式を異ならせ、コンテンツデータの方は時間を要せずに復号化できる暗号化方式とし、ヘッダ情報の方は復号化に多少時間を要しても暗号がもれないような複雑な暗号化方式とすることで、再生鍵データが含まれる情報部を今まで以上に知られにくくすると共に、再生タイミングに支障をきたすようなことがないようにしようというものである。

【0005】

【課題を解決するための手段】 本発明は、上記課題を解決するために、以下の1)～3)の手段より成る。すなわち、

1) 転送元端末から転送先端末に対して、そのデータ再生時の処理速度が所定の速度で要求される第1のデータと、それより遅い処理速度の再生が許される第2のデータとを含んで転送するデータの転送方法において、前記第1のデータを所定の第1の再生鍵を用いて暗号化すると共に、前記第2のデータを前記第1の再生鍵を用いて暗号化して復号化するときの処理速度より復号化に時間を要する第2の再生鍵を用いて暗号化し、これら暗号化された第1と第2のデータを転送するようにしたことを特徴とするデータの転送方法。

2) 前記データの転送方法は、販売元端末より販売先端末にコンテンツデータを配信するコンテンツ販売システムのデータ転送方法であり、前記第1のデータは、少なくとも実データであるコンテンツデータであり、前記第2のデータは少なくとも前記コンテンツデータに付加されるヘッダ情報であり、前記第1の再生鍵による暗号化は、所定バイト数の乱数で生成された前記第1の再生鍵と前記コンテンツデータとをXOR演算により暗号化し、前記第2の再生鍵による暗号化は、所定バイトの乱数で生成された第2の再生鍵により前記第2のデータがD

ES暗号化されたものであることを特徴とするコンテンツ販売システムのデータ転送方法。

3) 請求項1又は2記載の転送方法により転送されたデータを所定の領域に記録したことを特徴とする記録媒体。

【0006】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。図1は本発明が採用される販売店端末（キオスク端末）を経由するコンテンツ販売システムの一例を示す構成図、図2は図1のプレーヤに配信される販売ヘッダの構成を示す説明図、図3は図1のオーサリングシステムにより付与される販売ヘッダの構成を示す説明図、図4は図1のプレーヤに販売サブヘッダの構成を示す説明図である。

【0007】図1はコンテンツ販売システムの一例として、JRの売店（以下、キオスク）に販売店端末（以下、キオスク端末）5を設置した販売店設置端末経由方式のシステムを示している。まず、ホスト側では非圧縮の音楽コンテンツをオーサリングシステム1により例えばTwin VQ方式で圧縮し、次いでこの圧縮データを詳細の後述する再生鍵データで暗号化する。また、オーサリングシステム1ではこの再生鍵データを1次暗号化してこの1次暗号化再生鍵データと暗号化コンテンツを所定のデータ構造として記録し送信サーバ2、アップリンクセンタ3、衛星4を介してキオスク端末5のサーバに転送する。なお、この販売店設置端末経由方式のシステムでは、コンテンツを衛星4を介してキオスク端末5へ供給する代わりに、別の又は過渡的な供給方法として、記録済サーバを物流により定期的に交換するようにしてもよく、これに限られるものではない。さらに、販売店設置端末はキオスクの他、コンビニエンス・ストアなどの他の販売店に設置するようにしても良い。

【0008】キオスク端末5は、1次暗号化再生鍵データを2次暗号化してこの2次暗号化再生鍵データと暗号化コンテンツをプレーヤ（図中プレイヤーと示すこともある）6aにダウンロードする。このとき、キオスク端末5とプレーヤ6aの間はIEEE1394インタフェースを介して接続され、プレーヤ6aはダウンロード前にあらかじめ自己のIDをキオスク端末5に転送する。また、コピー元プレーヤ6aとコピー先プレーヤ6b間では、2次暗号化再生鍵データと暗号化コンテンツが再転送可能であり、この場合にもコピー先プレーヤ6bは再転送前にあらかじめ自己のIDをコピー元プレーヤ6aに転送する。このシステムの課金方式では、ユーザがプリペイド方式で電子チケットを購入することにより残高がプレーヤ6a内の電子財布に記憶され、また、課金情報がプレーヤ6aから決済ボックス7を介して課金管理サーバ8に転送される。この課金管理サーバ8は、キオスク端末5や後述のWebサーバ9を通じて前記の課金情報や各プレーヤ6a、6bの転送履歴を回収して、

これらの情報をもとに著作権管理等を行うようにしている。

【0009】また、この販売システムは、前述のキオスク端末を経由するシステムであると共に、インターネット方式により販売する経路も有している。図2は、そのインターネット方式による販売システムを示す図である。まず、ホスト側では販売店設置端末経由方式と同様に、非圧縮の音楽コンテンツをオーサリングシステム1により例えばTwin VQ方式で圧縮し、次いでこの圧縮データを再生鍵データで暗号化する。また、オーサリングシステム1ではこの再生鍵データを1次暗号化してこの1次暗号化再生鍵データと暗号化コンテンツを所定のデータ構造として記録し送信サーバ2、Webサーバ（インターネットサービス用サーバ）9に転送する。

【0010】Webサーバ9は1次暗号化再生鍵データを2次暗号化して2次暗号化再生鍵データと暗号化コンテンツをインターネットサービス用PCクライアント10（PCクライアントともいう）を介してプレーヤ6aにダウンロードする。このとき、Webサーバ9とPCクライアント10の間がダイヤルアップ接続により接続されるとともに、PCクライアント10とプレーヤ6aの間がIEEE1394インタフェースを介して接続され、また、プレーヤ6aはダウンロード前にあらかじめ自己の端末IDをPCクライアント10を介してWebサーバ9に転送する。また、同様に、コピー元プレーヤ6aとコピー先プレーヤ6b間で2次暗号化再生鍵データと暗号化コンテンツが再転送可能であり、この場合にもコピー先プレーヤ6bは再転送前にあらかじめ自己のIDをコピー元プレーヤ6aに転送する。また、ユーザがプリペイド方式で電子チケットを購入することにより残高がプレーヤ6a内の電子財布に記憶され、課金情報がプレーヤ6aからPCクライアント10、Webサーバ9を介して課金管理サーバ8に転送される。

【0011】プレーヤ6a、6bに転送されるフォーマットは、販売店設置端末経由のシステムとインターネット経由のシステムにおいて共通であって、販売コンテンツ毎に販売ヘッダと、販売サブヘッダと暗号化コンテンツデータを含み、販売サブヘッダは販売コンテンツ内の曲目数N毎に付与される。暗号化コンテンツデータはコンテンツヘッダ、サウンドストリーム（音楽コンテンツ）、テキストデータ（曲名、アーティスト名など）、拡張データなどを含む。

【0012】販売ヘッダは図3に示すように、販売コンテンツ内の曲目数Nに応じて可変長（ $=64N+M$ バイト（Bytes））であって、

- ・1バイトの販売ヘッダバージョンと、
- ・1バイトの販売ヘッダサイズと、
- ・1バイトの保留（Reserved）データと、
- ・1バイトの転送制御データと、
- ・8バイトのコンテンツ販売IDと、

- ・ 8バイトの転送元IDと、
- ・ 2バイトの販売チケット数と、
- ・ 1バイトの販売サブヘッダ数と、
- ・ 1バイトのコンテンツ曲数と、
- ・ 32バイトの制作タイトル名と、
- ・ 16バイトの制作会社名と、
- ・ $4 \times N$ バイトの曲目毎のデータ長と、
- ・ $8 \times N$ バイトの曲目毎の曲名と、
- ・ $8 \times N$ バイトの曲目毎のアーティスト名と、
- ・ $4 \times N$ バイトの曲目毎の演奏時間と、
- ・ Kバイト ($64N + M - K$ バイト目 $\sim 64N + M$ バイト目) の再生鍵データ (暗号化データ) を含む。

【0013】これに対し、図4はオーサリングシステム1によりマスタリング時に付与される販売ヘッダの構成を示し、この販売ヘッダは図2に示すデータの他に、制作タイトル名、N曲分の曲名、N曲分のアーティスト名、N曲分のISRC (International Standard Recording Code) を含む。

【0014】販売サブヘッダは図5に詳しく示すように、

- ・ 1バイトのサブヘッダバージョンと、
- ・ 1バイトのサブヘッダサイズと、
- ・ 1バイトの保留 (Reserved) データと、
- ・ 1バイトの転送制御データと、
- ・ 8バイトのコンテンツ販売IDと、
- ・ 8バイトの転送元IDと、
- ・ 2バイトの販売チケット数と、
- ・ 1バイトの指定曲番と、
- ・ 32バイトの制作タイトル名と、

を含む。

【0015】前記の販売ヘッダ及び販売サブヘッダ内の転送制御データは図6に詳しく示すように、4ビットb0～b3の再転送世代数データと4ビットb4～b7の再転送禁止/許可データを含む。

・ 再転送世代数ビットb0～b3

0000: 再転送禁止

0001～1111: 再転送世代数 (再転送許可)

著作権者 (ホスト) 側が設定して再転送毎にカウントダウンし、0000で再転送禁止

・ 再転送禁止/許可ビットb4～b7

0000: 再転送許可

0001: 再転送禁止

0010～1111: 保留 (Reserved)

【0016】また、前述のオーサリングシステム1における暗号化処理は次のように行われる。図7は、その処理を説明するためのフローチャートである。まず、販売ヘッダ毎に所定バイトの再生鍵データを乱数で作成し (ステップS1)、次いで販売コンテンツデータをコンテンツヘッダ、サウンドストリーム (音楽コンテンツ)、テキストデータ (曲名、アーティスト名など)、

拡張データの各領域毎に分けて、上記の再生鍵データ (乱数) と所定バイトずつに排他的論理和 (XOR) 演算することにより、販売コンテンツデータを各領域毎に独立して暗号化する (ステップS2)。

【0017】また、(販売ヘッダの指定項目順の文字列) + (販売サブヘッダの指定項目順の文字列) の合成文字列に基づいてハッシュ関数 (MD5) により所定バイトのハッシュ値を作成し (ステップS3)、次いで上記の再生鍵データとハッシュ値をXOR演算することにより1次暗号化再生鍵データを作成する (ステップS4)。そして、1次暗号化再生鍵データを販売ヘッダの再生鍵データ領域に格納して暗号化コンテンツとともに販売元端末 (キオスク端末5、Webサーバ9) に伝送する (ステップS5)。このように、ステップS3とS4により販売ヘッダに基づく情報により再生鍵データを暗号化することにより販売ヘッダとコンテンツデータの組み合わせを改ざんした場合には復号できないようにしている。

【0018】また、図8は販売元端末 (キオスク端末5、Webサーバ9) の再生鍵の2次暗号化の処理フローを示し、まず、1次暗号化再生鍵データを転送先プレーヤIDを鍵としてDES暗号化して転送先プレーヤ6aの2次暗号化再生鍵データを作成し (ステップS11)、次いでこの2次暗号化再生鍵データを暗号化コンテンツとともに販売先端末 (プレーヤ6a) に伝送する処理となっている (ステップS12)。

【0019】また、図9は販売先端末 (転送先プレーヤ6a) の暗号化された再生鍵及びコンテンツデータの復号処理方法の処理フローを示している。まず、2次暗号化再生鍵データを自己のプレーヤIDを鍵としてDES復号することにより1次暗号化再生鍵データに復号するとともに (ステップS21)、(販売ヘッダの指定項目順の文字列) + (販売サブヘッダの指定項目順の文字列) の合成文字列に基づいてハッシュ関数 (MD5) により所定バイトのハッシュ値を作成する (ステップS22)。次いでこれらの1次暗号化再生鍵データとハッシュ値をXOR演算することにより元の再生鍵データに復号し (ステップS23)、次いで暗号化販売コンテンツデータを所定バイトずつ元の再生鍵データとXOR演算することにより元の販売コンテンツデータに復号し、これを伸長して再生する (ステップS24)。

【0020】特に、本システムの暗号化方式では、コンテンツデータやテキストデータなどの実データをXOR演算で暗号化し、ヘッダ等の実データと異なるデータはDES暗号化方式で暗号化している。これは、再生時の処理速度に対応しているもので、再生時に処理速度が速く要求される実データは復合化のことを考慮して複合化が速く行えるXOR暗号化方式を採用し、それほどの処理速度が要求されないヘッダ情報には、それより復号化に時間を要する複雑なDES暗号化方式として、再生速

度とデータの流出との両方を考慮した暗号化としている。

【0021】また、前記のプレーヤ6a、6bは、図10に示す構成で、プレーヤ6aの符号のみを用いて説明する。プレーヤ6aは、データ転送インターフェース6a-1、電子財布部6a-2、表示部6a-3、操作部6a-4、記憶部6a-5、暗号化/復号化部6a-6、データ圧縮/伸長部6a-7、再生部6a-8、出力端子6a-9、制御部6a-10及び内部バス6a-11から構成されている。

【0022】データ転送インターフェース6a-1は、送信側プレーヤと受信側プレーヤとの間、これらプレーヤとキオスク端末5との間、又は、後述のPCクライアント（パソコン）とのデータ転送に使用される。電子財布部6a-2は、電子マネーの受け取り、支払いをすることができる。プリペイド方式により電子マネーを予めデポジットしておき、その電子マネーをコンテンツ料金に応じて減額するようにしている。後述の説明では、プリペイド方式による説明としているが、周知のクレジット方式としても良い。

【0023】表示部6a-3は、電子財布の電子マネーの残額や、端末間のデータ送受信時の送受信状況、コンテンツ再生時の再生状況、コピーの可否等を表示する。操作部6a-4は、複数のデータの中から再生したいデータを探し出すためのデータ頭出し操作、再生時の再生音量操作等に使用される。記憶部6a-5には、キオスク端末5から受け取ったヘッダ情報やコンテンツデータや再生、他の携帯端末等から受け取ったヘッダ情報やコンテンツデータ等が記憶される。

【0024】暗号化/復号化部6a-6は、認証データの生成やコンテンツデータ、再生鍵及びヘッダ情報の暗号化又は復号化を行う。データ圧縮/伸長部6a-7は、データを圧縮、又は圧縮されているデータを伸長する。転送されるデータは、転送効率を上げるため圧縮状態とする。従って、データ送信前にデータを圧縮し、データ受信後に必要に応じて圧縮データを伸長する。再生部6a-8は、コンテンツデータから音声、テキストデータ等を再生する。再生された音声等は、出力端子6a-9から外部に出力される。制御部6a-10は、上記各部の制御や、履歴転送回数、コンテンツ販売ID、転送元ID及び転送制御データの履歴数分の登録等を内部の記憶部mに行わせる。

【0025】次に、各端末間の処理手順につき順次詳述していく。まず、図11、図12はキオスク端末（ホスト側）5とプレーヤの間の転送手順を示している。図5においてキオスク端末5と例えば上記構成のプレーヤ6aがIEEE1394インタフェースを介して接続された状態である。また、図11以下の図中、「Form 1」、「Form 2」…などは信号フォーマットの番号を示すもので、詳細な説明は省略するが、前述の販売店設置端末経由のシステムとインターネット経由のシステムにおいて

共通であって、基本的には図13に示すように、発信元コード（図14に示すシステム構成装置の種類を示すコード）と、コマンドコード（図15、図16参照）と、データ長と実データ（暗号化データ）により構成されている。ただし、転送元（キオスク端末5、Webサーバ9）からプレーヤ6aに送信される各種の「要求」や、プレーヤ6aから転送元5、9に送信される各種の「通知」のフォーマットは、実データは含まれず、発信元コードと、コマンドコードと、データ長（=オール0）のみにより構成されている。

【0026】キオスク端末5内において、このキオスク端末5内には図示はしていないが、データ転送インターフェース、表示部、記憶部、暗号化/復号化部、再生部、出力端子、制御部、内部バスなど、プレーヤ6a、6bとほぼ同様の機能部が含まれている。まず、図示しない暗号化部において例えば8バイトの乱数認証データD1を作成し、決済ボックス、キオスク端末、各プレーヤ、Webサーバ9及びPCクライアント10において共通に保持している共通鍵K1~K6の一つである共通鍵データK1によりDES暗号化し、この暗号化された認証Aデータを8バイトの所定の送信フォーム「1」（図中「Form 1」と示される）のプレーヤ認証AデータD1としてデータ転送インターフェース介してプレーヤ6aに送信する。

【0027】プレーヤ6aでは、このプレーヤ認証AデータD1をデータ転送インターフェース6a-1を介して受信し、暗号化/復号化部6a-6において、共通鍵データK1によりDES復号化し、この復号化で得られた認証AデータD1を他の共通鍵データK2によりDES暗号化し、返信プレーヤ認証Aデータを作成する。それと同時に、8バイトの乱数認証AデータD3を作成し、この認証AデータD3を他の共通鍵データK3によりDES暗号化し、このデータをホスト認証Aデータとし、所定の送信フォーム「2」でホスト認証Aデータと前記返信プレーヤ認証Aデータとを再びキオスク端末5に返信する。

【0028】キオスク端末5では、データ転送インターフェースを介して返信プレーヤ認証Aデータとホスト認証Aデータとを受信し、これらを暗号化/復号化部に供給し、ここで、返信プレーヤ認証Aデータを共通鍵データK3によりDES復号化し、この復号化された認証AデータD1と送信認証AデータD1とが制御部において照合される。照合の結果、不一致の場合には、このキオスク端末5側において行った前述の処理を2回まで再度実行する。それでも不一致する場合にはキオスク端末5における処理を中止する。

【0029】また、一方、一致の場合には、受信ホスト認証Aデータを共通鍵データK3によりDES復号化し、この復号化で得られた認証AデータD2を、他の共通鍵データK4によりDES暗号化し、返信ホスト認証

Aデータとし、このデータを所定のフォーム「3」でプレーヤ6aに送信する。プレーヤ6aの暗号化/復号化部6a-6では、この返信ホスト認証Aデータを共通鍵データ4によりDES復号化し、復号化された認証AデータD2を得て、この復号化された認証AデータD2と送信ホスト認証Aデータとを制御部6a-10において照合し、一致の場合には所定の送信フォーム「4」でホスト認証をキオスク端末5に送信し、その後の処理を受け付ける。また、一方、認証不一致の場合には、フォーム「4」の認証不可をキオスク端末5に送信し、これ以降の処理の受付を禁止する。

【0030】次に、キオスク端末5からプレーヤ6aに対し、所定の送信フォーム「5」のプレーヤIDの送信要求がなされる。これを受信したプレーヤ6b側では暗号化/復号化部6a-7において、自己プレーヤIDをホスト認証に使用した認証AデータD2を鍵として16バイトづつDES暗号化し、このデータを所定の送信フォーム「6」でキオスク端末5に送信する。キオスク端末5における暗号化/復号化部ではホスト認証AデータD2を鍵として16バイトづつ復号化し、復号化したプレーヤIDを記憶部に保存する。また、プレーヤ6aからのプレーヤIDの送信がない場合には、再度、プレーヤIDの要求をし、それでも送信がない場合には、プレーヤへの処理を中止する。

【0031】次いでキオスク端末5がプレーヤ6aに対して所定の送信フォーム「7」の転送履歴送信要求を送信すると、プレーヤ6aでは、制御部6a-10内の記憶部6amに前述の受信した履歴数、履歴転送回数、コンテンツ販売ID、転送元ID、転送制御データ等の転送履歴が有るか否かを検出し、有る場合には暗号化/復号化部6a-6で販売コンテンツ受信順に全転送履歴をホスト認証AデータD2を鍵としてDES暗号化し、キオスク端末5に対して所定の送信フォーム「8」で転送履歴を送信し、キオスク端末5では、受信した転送履歴をホスト認証AデータD2を鍵としてDES復号化する。次いでキオスク端末5がプレーヤ6aに対して所定の送信フォーム「9」の転送履歴削除要求を送信すると、プレーヤ6aでは転送履歴を削除する。また、転送履歴削除要求が無い場合には、全転送履歴の履歴転送回数を1カウントアップして保存する。そして、プレーヤ6aが転送履歴を削除した場合にはキオスク端末5に対して所定の送信フォーム「10」の転送履歴削除通知を送信する。従って、これらの転送履歴は、後に課金管理サーバ8に供給され、そこで著作権管理のための情報等に使用される。

【0032】次いでキオスク端末5における操作に応じて「コンテンツ転送」、「編集データ転送」に選択的に移行する。「コンテンツ転送」が選択された場合には、キオスク端末5がプレーヤ6aに対し、所定の送信フォーム「11」のチケット残高送信要求がなされる。プレ

ーヤ6aの制御部6a-10では電子財布6a-2におけるチケットの残高を照合し、この残高を暗号化/復号化部6a-6においてホスト認証に使用した認証AデータD2を鍵として16バイトづつDES暗号化して、このデータを送信フォーム「12」によりキオスク端末5に送信し、キオスク端末5の暗号化/復号化部でホスト認証で受信した認証AデータD2を鍵として16バイトづつDES復号化し、チケット残高を記憶部に保存する。このとき、残金のない場合には、処理を中止するか、クレジット方式の場合にはその情報を課金管理サーバ8に送信して周知の手続き処理が行われる。チケット残高の受信が得られない場合には、再度前述の残高送信要求の処理を実行し、送信がない場合にはプレーヤ処理を中止する。

【0033】前記の処理において、残高送信があった場合には、次いでプレーヤ6aに送信フォーム「15」の空き容量送信要求をする。プレーヤ6aでは記憶部6a-5内に記憶されているデータのヘッダー/コンテンツ空き容量を照合して、キオスク端末5に送信フォーム「16」によりその照合結果を送信する。キオスク端末5ではこの空き容量を記憶部に記憶する。空き容量がない場合には処理を中止するか、キオスク端末側で空き容量を確保するための制御信号を出力することになる。また、送信がない場合には前述の処理を再度実行し、それでも送信がない場合にはプレイ処理を中止する。

【0034】次いでキオスク端末5からプレーヤ6aに所定の送信フォーム「17」の内蔵コンテンツ販売IDの送信要求を行う。プレーヤ6aにおける記憶部6a-5内に内蔵コンテンツ販売IDが記録されている場合には、全コンテンツ販売IDをホスト認証に使用した認証AデータD2を鍵として16バイトづつDES暗号化し、このデータを所定の送信フォーム「18」によりキオスク端末5に送信する。内蔵コンテンツ販売IDが無い場合にはその旨を所定の送信フォーム「18」により送信する。

【0035】次いでキオスク端末5がプレーヤ6aに対して所定の送信フォーム「19」、「20」、「21」でそれぞれ販売ヘッダ、販売サブヘッダ、コンテンツデータを順次を送信すると、プレーヤ6aがこれらにตอบสนองしてキオスク端末5に対して所定の送信フォーム「22」の各データ受信通知を送信する。次いでキオスク端末5では、記憶部に記憶されている販売ヘッダ内の1次暗号化再生鍵データを先に送信されてきたプレーヤ6aのプレーヤIDを鍵として2次暗号化し、この2次暗号化鍵データをプレーヤ6aに対して所定の送信フォーム「25」で送信する。プレーヤ6aでは、この2次暗号化鍵データを記憶部6a-5の販売ヘッダの鍵データ保存領域に格納する。そして、電子財布部6a-2により販売チケット数分減額し、受信コンテンツの転送履歴を制御部6a-10内の記憶部mに記録する。そして、これらの

処理が終了すると、所定の送信フォーム「26」の再生鍵データ受信通知をキオスク端末5に送信し、キオスク端末5とプレーヤ6aの間のIEEE1394インタフェースを切断する。

【0036】また、一方、図17は、前記の「コンテンツ転送」の代わりに「編集データ転送」が選ばれたときのフローチャートで、同図に示すように、このモードが選択されると、キオスク端末5がプレーヤ6aに対して所定の送信フォーム「30」の編集データ送信要求を送信すると、プレーヤ6aがこれに応答して編集対象の曲を、十進数で1から始まる再生順番、その曲データ長、曲名、アーティスト名の順に、所定の送信フォーム「31」でキオスク端末5に送信する。次いでキオスク端末5ではこの送信データを記憶部に保存し、プレーヤ6aに対して所定の送信フォーム「32」のコンテンツ削除データを送信する。プレーヤ6aではこのデータに基づいて受信削除再生順番の曲の再生リストからの削除、及び販売コンテンツデータと販売サブヘッダの消去、販売ヘッダの再転送禁止処理又は消去を行う。そして、キオスク端末5に対して所定の送信フォーム「33」の販売コンテンツデータ削除通知を送信する。次いでキオスク端末5がプレーヤ6aに対して所定の送信フォーム「15」の空き容量送信要求を送信すると、プレーヤ6aがこれに応答してキオスク端末5に対して所定の送信フォーム「16」の空き容量を送信する。

【0037】次いでキオスク端末5は、前記の編集対象のデータに基づいて、再生順番の並び替え等の編集を行い、この編集済みデータをプレーヤ6aに対して所定の送信フォーム「34」で送信する。プレーヤ6aでは、これに基づき旧再生順番を新再生順番に変更し、その後、キオスク端末5に対して所定の送信フォーム「35」の編集済データ受信通知をプレーヤ6aに送信する。そして、キオスク端末5とプレーヤ6aの間のIEEE1394インタフェースを切断する。

【0038】次に、前述のインターネット方式におけるWebサーバ9とPCクライアント10の間、及びPCクライアント10とプレーヤ6aの間の通信手順につき、図18～図23を参照して説明する。まず、図18に示すようにPCクライアント10とプレーヤ6aがIEEE1394インタフェースを介して接続されると、PCクライアント10がプレーヤ6aに対して所定の送信フォーム「38」のプレーヤ認証Bデータを送信し、プレーヤ6aがこれに応答してPCクライアント10に対して所定の送信フォーム「39」の返信プレーヤ認証Bデータとホスト認証Bデータを送信する。次いでPCクライアント10がプレーヤ6aに対して所定の送信フォーム「40」の返信ホスト認証Bデータを送信すると、プレーヤ6aがこれに応答してPCクライアント10に対して所定の送信フォーム「41」のホスト認証B結果を送信する。

【0039】次いでPCクライアント10がプレーヤ6aに対して所定の送信フォーム「11」のチケット残高送信要求を送信すると、プレーヤ6aがこれに応答してPCクライアント10に対して所定の送信フォーム「12」のチケット残高を送信する。次いでPCクライアント10がプレーヤ6aに対して所定の送信フォーム「15」のメモリの空き容量送信要求を送信すると、プレーヤ6aがこれに応答してPCクライアント10に対して所定の送信フォーム「16」の空き容量を送信する。次いでPCクライアント10がプレーヤ6aに対して所定の送信フォーム「17」の、メモリに既にダウンロードされて記憶されている内蔵コンテンツ販売IDの送信を要求すると、プレーヤ6aがこれに応答してPCクライアント10に対して所定の送信フォーム「18」の内蔵コンテンツ販売IDを送信する。次いで所定のフォーム「34」、「35」により前記の図17における販売キオスクとプレーヤ間における同様の編集データの要求と送信が行われる。次いでユーザなどがPCクライアント10を介して指示することにより、「コンテンツ選択・購入」、「チケット購入」、「コンテンツ編集・削除」の各処理に選択的に移行する。

【0040】尚、前述のPCクライアント10とプレーヤ6aにおける認証方式は、前述の図11で説明したキオスク端末5とプレーヤ6aにおける処理とほぼ同様で、その相違する点は認証データの生成方法で、共通鍵データK5を用いて暗号化された返信プレーヤ認証Bデータを生成する点と、共通鍵データK6を用いて返信ホスト認証Bデータを生成する点である。前述の場合では認証Aデータを用いて互いの機器を認証するようにしたが、特に、この場合のPCクライアント10間との認証データは、データの流出が懸念されることから他とは異なる認証データを用いている。従って、更に他の機器間で認証データの流出が懸念されるようなら、他の機器毎に認証データを異ならせても良い。

【0041】また、一方、「コンテンツ選択・購入」が選択された場合には、図19に示すようにクライアント10とプレーヤ6aの間で上記の「チケット残高」、「空き容量」及び「内蔵コンテンツ販売ID」のやり取りを再度行う。次いでクライアント10がサーバ9に対してコンテンツ購入要求情報を送信し、次いでサーバ9がクライアント10に対して販売内容チェック結果を送信する。尚、前記の残高送信データや内蔵コンテンツIDを送信するときには、ホスト認証Bデータを鍵としてDES暗号化するようにしている。

【0042】次いでクライアント10がWebサーバ9に対してコンテンツ購入要求を送信すると、Webサーバ9がクライアント10に対してプレーヤ認証Aデータを送信し、次いでクライアント10がプレーヤ6aに対してこのプレーヤ認証Aデータを送信する。次いでプレーヤ6aがこれに応答してクライアント10に対して返

信プレーヤ認証Aデータとホスト認証データを送信し、次いでクライアント10がWebサーバ9に対してこの返信プレーヤ認証Aデータとホスト認証Aデータを送信する。

【0043】次いでサーバ9がクライアント10に対して返信ホスト認証A送信データを送信し、次いでクライアント10がプレーヤ6aに対してこの返信ホスト認証A送信データを送信する。次いでプレーヤ6aがこれに回答してクライアント10に対して返信ホスト認証Aデータの結果を送信し、次いでクライアント10がサーバ9に対してこの結果を送信する。

【0044】次に、図20に示すように、Webサーバ9がPCクライアント10に対して所定の送信フォーム「5」、「11」、「15」、「17」、「7」でそれぞれプレーヤID送信要求、チケット残高送信要求、空き容量送信要求、内蔵コンテンツ販売ID送信要求、転送履歴送信要求を送信する。次いでPCクライアント10がプレーヤ6aに対して所定の送信フォーム「5」のプレーヤID送信要求を送信するとプレーヤ6aがこれに回答してPCクライアント10に対して所定の送信フォーム「6」のプレーヤIDを送信し、PCクライアント10がプレーヤ6aに対して所定の送信フォーム「11」のチケット残高送信要求を送信するとプレーヤ6aがこれに回答してPCクライアント10に対して所定の送信フォーム「12」のチケット残高を送信する。

【0045】また、PCクライアント10がプレーヤ6aに対して所定の送信フォーム「15」の空き容量送信要求を送信するとプレーヤ6aがこれに回答してPCクライアント10に対して所定の送信フォーム「16」の空き容量を送信し、PCクライアント10がプレーヤ6aに対して所定の送信フォーム「17」の内蔵コンテンツ販売ID送信要求を送信するとプレーヤ6aがこれに回答してPCクライアント10に対して所定の送信フォーム「18」の内蔵コンテンツ販売IDを送信し、PCクライアント10がプレーヤ6aに対して所定の送信フォーム「7」の転送履歴送信要求を送信するとプレーヤ6aがこれに回答してPCクライアント10に対して所定の送信フォーム「8」の転送履歴を送信する。PCクライアント10はWebサーバ9に対して、これらの所定の送信フォーム「6」、「12」、「16」、「18」、「8」でそれぞれプレーヤID、チケット残高、空き容量、内蔵コンテンツ販売ID、転送履歴を送信する。そして、この転送履歴は前述したように課金管理サーバ8に送信されることになる。

【0046】次いでWebサーバ9が転送履歴を回収すると、PCクライアント10に対して所定の送信フォーム「9」の転送履歴削除要求を送信するとPCクライアント10がプレーヤ6aに対してこの送信フォーム「9」の転送履歴削除要求を送信し、プレーヤ6aがこれに回答して制御部6a-10内の記憶部mに記憶されて

いる転送履歴を削除する。そして、PCクライアント10に対して所定の送信フォーム「10」の転送履歴削除通知を送信するとPCクライアント10がWebサーバ9に対してこの送信フォーム「10」の転送履歴削除通知を送信する。これらのデータの送信は、プレーヤ6aにおいて、空き容量の送信を除き、ホスト認証Aデータを鍵としてDES暗号化されて送信される。

【0047】次いでWebサーバ9がPCクライアント10に対して送信フォーム「19」、「20」、「21」でそれぞれ販売ヘッダ、販売サブヘッダ、販売コンテンツデータを送信する。次いでPCクライアント10がプレーヤ6aに対して送信フォーム「19」、「20」、「21」でそれぞれ販売ヘッダ、販売サブヘッダ、販売コンテンツデータを送信するとプレーヤ6aは、これらのデータを記憶部6a-5に記憶する。そして、PCクライアント10に対して送信フォーム「22」の各データ受信通知を送信し、PCクライアント10がこれに対してこの送信フォーム「22」のデータ受信通知を送信する。

【0048】次いで図21に示すようにWebサーバ9がPCクライアント10に対して送信フォーム「25」の再生鍵データを送信すると、PCクライアント10がプレーヤ6aに対してこの送信フォーム「25」の再生鍵データを送信する。次いでプレーヤ6aは、受信再生鍵データを販売ヘッダの鍵データ保存領域に格納すると共に、購入チケット数分の減額、受信コンテンツデータの転送履歴等の記録を行いPCクライアント10に対して送信フォーム「26」の再生鍵データ受信通知を送信し、PCクライアント10がWebサーバ9に対してこの送信フォーム「26」の再生鍵データ受信通知を送信する。そして、PCクライアント10とプレーヤ6aの間のIEEE1394インタフェースを切断する。

【0049】次に、図18において「コンテンツ編集・削除」が選択された場合につき、図22を参照して説明する。この処理では、サーバ9とクライアント10の間の回線は接続されず、クライアント10とプレーヤ6aの間のみが接続された状態で行われる。まず、クライアント（ホスト側）10がプレーヤ6aに対してコンテンツ削除データを送信すると、プレーヤ6aがこれに基づいて図17のプレーヤ処理11と同様にしてデータの削除をする。そして、クライアント10に対してコンテンツ削除通知を送信する。

【0050】次に、ここで、クライアント10において、編集処理が行われる。その処理を図23を参照して説明する。まず、プレーヤ6aから転送された編集対象のコンテンツを表示し（ステップS1）、次いで編集項目が入力されると（ステップS2）、入力項目に応じて編集対象のコンテンツを編集する（ステップS3）。そして、図22に示すように、前記の編集済データが送信されると、プレーヤ6aがこれに回答してクライアント

10に対して編集済データ受信通知を送信する。

【0051】次に、図24～図26を参照して図19～図21に対応した別の「コンテンツ選択・購入」の実施例につき説明する。すなわち、図18において、「コンテンツ選択・購入」が選択された場合には、図24に示すようにクライアント10がサーバ9に対してコンテンツ購入要求情報を送信し、次いでサーバ9がクライアント10に対して販売内容チェック結果を送信する。次いでクライアント10がサーバ9に対してコンテンツ購入要求を送信すると、サーバ9がプレーヤ認証Aデータをクライアント10をスルーしてプレーヤ6aに送信し、プレーヤ6aがこれに回答して返信プレーヤ認証Aデータとホスト認証データをクライアント10をスルーしてサーバ9に送信する。次いでサーバ9が返信ホスト認証A送信データをクライアント10をスルーしてプレーヤ6aに送信すると、プレーヤ6aがこれに回答して返信ホスト認証A送信データの結果をクライアント10をスルーしてサーバ9に送信する。

【0052】次に、図25に示すように、サーバ9がプレーヤID送信要求、チケット残高送信要求、空き容量送信要求、内蔵コンテンツ販売ID送信要求、転送履歴送信要求をクライアント10をスルーしてプレーヤ6aに送信すると、プレーヤ6aがこれに回答してプレーヤID、チケット残高、空き容量、内蔵コンテンツ販売ID、転送履歴をクライアント10をスルーしてサーバ9に送信する。

【0053】次いでサーバ9が転送履歴削除要求をクライアント10をスルーしてプレーヤ6aに対して送信すると、プレーヤ6aがこれに回答して転送履歴削除通知をクライアント10をスルーしてサーバ9に送信する。次いでサーバ9が販売ヘッダ、販売サブヘッダ、販売コンテンツデータをクライアント10をスルーしてプレーヤ6aに送信すると、プレーヤ6aがこれに回答して各データ受信通知をクライアント10をスルーしてサーバ9に送信する。次いで図26に示すようにサーバ9が再生鍵データをクライアント10をスルーしてプレーヤ6aに対して送信すると、プレーヤ6aがこれに回答して再生鍵データ受信通知をクライアント10をスルーしてサーバ9に送信する。そして、クライアント10とプレーヤ6aの間のIEEE1394インタフェースを切断する。

【0054】次に、図27を参照してプレーヤ6a、6b間におけるデータ転送の処理につき説明する。まず、プレーヤ（ホスト側）6aの暗号化部6a-5において例えば8バイトの乱数認証AデータD1を作成し、共通鍵データK1によりDES暗号化し、この暗号化された認証AデータD1を8バイトの所定の送信フォーム「1」でデータ転送インターフェース6a-1を介してプレーヤ6bに送信する。プレーヤ6bでは、このプレーヤ認証AデータD1をデータ転送インターフェース6b-1を介

して受信し、暗号化/復号化部6b-6において、共通鍵データK1によりDES復号化し、この復号化で得られた認証AデータD1を他の共通鍵データK2によりDES暗号化し、返信プレーヤ認証Aデータを作成する。それと同時に、8バイトの乱数認証AデータD3を作成し、この認証AデータD3を更に他の共通鍵データK3によりDES暗号化し、このデータをホスト認証Aデータとし、所定送信フォーム「2」でホスト認証Aデータと前記返信プレーヤ認証Aデータとを再びプレーヤ6aに返信する。

【0055】プレーヤ6aでは、データ転送インターフェース6a-1を介して返信プレーヤ認証Aデータとホスト認証Aデータとを受信し、これらを暗号化/復号化部6a-6に供給し、ここで、返信プレーヤ認証Aデータが共通鍵データK3によりDES復号化され、この復号化された認証AデータD1と送信認証AデータD1とが制御部6a-10において照合される。照合の結果、不一致の場合には、このプレーヤ6a側において行った前述の処理を2回まで再度実行する。それでも不一致する場合にはプレーヤ6aにおける処理を中止する。

【0056】また、一方、一致した場合には、受信ホスト認証Aデータを共通鍵データK3によりDES復号化し、この復号化で得られた認証データD2を、他の共通鍵データK4によりDES暗号化し、返信ホスト認証Aデータとし、このデータを所定の送信フォーム「3」によりプレーヤ6bに送信する。プレーヤ6bの暗号化/復号化部6b-6では、この返信ホスト認証Aデータを共通鍵データ4によりDES復号化し、復号化された認証AデータD2を得て、この復号化された認証AデータD2と送信ホスト認証Aデータとを制御部6b-10において照合し、一致の場合には所定の送信フォーム「4」のホスト認証をプレーヤ6aに送信し、その後の処理を受け付ける。また、一方、認証不一致の場合には、所定の送信フォーム「4」の認証不可をプレーヤ6aに送信し、これ以降の処理の受付を禁止する。

【0057】次いでプレーヤ6aからプレーヤ6bに対し、所定の送信フォーム「5」のプレーヤIDの送信要求がなされる。これを受信したプレーヤ6b側では暗号化/復号化部6b-7において、自己プレーヤIDをホスト認証に使用した認証AデータD2を鍵として16バイトづつDES暗号化し、所定の送信フォーム「6」でデータをプレーヤ6aに送信する。プレーヤ6aにおける暗号化/復号化部6a-6ではホスト認証AデータD2を鍵として16バイトづつ復号化し、復号化したプレーヤIDを記憶部mに保存する。また、プレーヤ6bからのプレーヤIDの送信がない場合には、再度、プレーヤIDの要求をし、それでも送信がない場合には、プレーヤ処理を中止する。

【0058】次いでプレーヤ6aからプレーヤ6bに対し、所定の送信フォーム「11」のチケット残高送信要

求がなされる。プレーヤ6bの制御部6b-10では電子財布6b-2におけるチケットの残高を照合し、この残高を暗号化／復号化部6b-6においてホスト認証に使用した認証AデータD2を鍵として16バイトづつDES暗号化して、このデータを送信フォーム「12」によりプレーヤ6aに送信し、プレーヤ6aの暗号化／復号化部6a-6でホスト認証で受信した認証AデータD2を鍵として16バイトづつDES復号化し、チケット残高を記憶部mに保存する。このとき、チケット残高の受信が得られない場合には、再度前述の残高送信要求の処理を実行し、送信がない場合にはプレーヤ処理を中止する。

【0059】残高送信があれば、次に、プレーヤ6bに所定の送信フォーム「15」の空き容量送信要求をする。プレーヤ6bでは記憶部6b-5内に記憶されているデータのヘッダー／コンテンツ空き容量を照合して、プレーヤ6aに所定の送信フォーム「16」によりその照合結果を送信する。プレーヤ6aではこの空き容量を記憶部mに記憶する。送信がない場合には前述の処理を再度実行し、それでも送信がない場合にはプレイ処理を中止する。

【0060】次いでプレーヤ6aからプレーヤ6bに所定の送信フォーム「17」の内蔵コンテンツ販売IDの送信要求を行う。プレーヤ6bにおける記憶部6b-5内にすでに転送済みの内蔵コンテンツ販売IDが記録されているには、全コンテンツ販売IDをホスト認証に使用した認証AデータD2を鍵として16バイトづつDES暗号化し、このデータを送信フォーム「18」によりプレーヤ6aに送信する。内蔵コンテンツ販売IDが無い場合には、その旨を所定の送信フォーム「18」により送信する。

【0061】プレーヤ6aでは、制御部6a-6において、記憶部6a-5に記憶されている転送コンテンツ販売IDとプレーヤ6bから送信されてきた内蔵コンテンツ販売IDとを照合する。同一コンテンツ販売IDがある場合にはプレーヤ6aの処理を中止する。また、同一コンテンツ販売IDが無い場合には、転送コンテンツ販売ヘッダ内の転送制御データ再転送世代数を確認する。確認の結果、転送世代数が「0000：コピー不可」である場合には、その旨を再生部6a-8を通じて表示部6a-3において、「コピー不可」を表示して処理を中止すると共に、プレーヤ6b側も所定時間内にデータの受信が得られないと同様に表示部6b-3に「コピー不可」を表示する。

【0062】また、転送世代数が「0001」以上である場合には、転送制御データの再転送世代数を1カウントダウンし、転送コンテンツの再生鍵データを除く販売ヘッダをプレーヤ6bの認証時に使用した認証AデータD1を鍵としてDES暗号化して、所定の送信フォーム「19」でプレーヤ6bに送信する。プレーヤ6bでは、これを受信し販売ヘッダを認証AデータD1を用い

てDES復号化し、記憶部6b-5に記憶すると共に、受信通知をプレーヤ6bに送信する。

【0063】また、プレーヤ6aでは、記憶部6a-5に販売サブヘッダがある場合には前記の販売ヘッダの場合と同様にプレーヤ6bの認証時に使用した認証AデータD1を鍵としてDES暗号化して、プレーヤ6aに対して所定の送信フォーム「20」で送信する。プレーヤ6aでは、この販売サブヘッダを認証AデータD1を鍵としてDES復号化し、記憶部6b-5に記憶する。また、プレーヤ6aに販売サブヘッダ情報が無い場合には、次の所定の送信フォーム「21」で前述の方式で暗号化されたコンテンツデータを送信する。プレーヤ6bでは、このコンテンツデータを記憶部6b-5に記憶し、所定の送信フォーム「22」で受信通知を返送する。

【0064】次いでプレーヤ6aでは、記憶部6b-5における転送販売ヘッダ再生鍵保存領域の2次暗号化再生鍵データを、暗号化／復号化部6a-6において自己プレーヤ(6a)のIDを鍵としてDES復号化し、1次暗号化再生鍵データを復号する。そして、この1次暗号化再生鍵データを、転送先であるプレーヤ6bのIDを鍵として再び2次DES暗号化処理を行い、この2次暗号化された再生鍵データを所定の送信フォーム「25」でプレーヤ6bに送信する。プレーヤ6bでは、この2次暗号化鍵データを記憶部6b-5の販売ヘッダの鍵データ保存領域に格納する。そして、電子財布部6b-2により販売チケット数分減額し、受信コンテンツの前述の転送履歴を制御部内6b-1の記憶部mに記録する。そして、これらの処理が終了すると、所定の送信フォーム「26」の再生鍵データ受信通知をプレーヤ6aに送信し、プレーヤ6aとプレーヤ6bの間のIEEE1394インタフェースを切断する。

【0065】次に、図28、図29は、前述のプレーヤ6a及びプレーヤ6b間におけるデータ転送の別の実施例で、前述の実施例と異なる点は、特に、プレーヤ6bから転送履歴をもらう点である。所定の送信フォーム「1」～「6」までは、前述の実施例である図27の説明と同一であるため説明を省略し、送信フォーム「7」より説明する。この送信フォーム「7」により、プレーヤ6aからプレーヤ6bに対して転送履歴の要求を行う。プレーヤ6bでは、制御部6b-10内の記憶部mに転送履歴が有るか否かを検出し、有る場合には暗号化／復号化部6b-6で販売コンテンツ受信順に全転送履歴をホスト認証AデータD2を鍵としてDES暗号化し、応答してプレーヤ6aに対して所定の送信フォーム「8」で転送履歴を送信し、プレーヤ6aでは、暗号化／復号化部6a-6において転送履歴をホスト認証AデータD2を鍵としてDES復号化する。そして、制御部6a-10では、これらのデータに基づきコピーが可能な否かをチェックし、その旨を所定のフォーム「9」でプレーヤ6bに送信する。プレーヤ6bでは、特に、コピーができ

ない場合には、再生部6b-8を通じて表示部6b-3によりその旨を表示する。また、コピー可の場合には全転送履歴の履歴転送回数を1カウントアップして保存する。そして、所定の送信フォーム「10」により前記のデータの受信をプレーヤ6aに送信する。

【0066】そして、コピー可と判断された場合には、「コンテンツ転送」処理へと進行し、プレーヤ6aからプレーヤ6bに対し、所定の送信フォーム「11」のチケット残高送信要求がなされる。プレーヤ6bの制御部6a-10では電子財布6b-2におけるチケットの残高を照合し、この残高を暗号化／復号化部6b-6においてホスト認証に使用した認証AデータD2を鍵として16バイトづつDES暗号化して、このデータを送信フォーム「12」によりプレーヤ6aに送信し、プレーヤ6aの暗号化／復号化部6a-6でホスト認証で受信した認証AデータD2を鍵として16バイトづつDES復号化し、チケット残高を記憶部6a-5に保存する。このとき、チケット残高の受信が得られない場合には、再度前述の残高送信要求の処理を実行し、送信がない場合にはプレーヤ処理を中止する。

【0067】前記の処理において、残高送信があった場合には、次に、プレーヤ6bに送信フォーム「15」の空き容量送信要求をする。プレーヤ6bでは記憶部m内に記憶されているデータのヘッダー／コンテンツ空き容量を照合して、プレーヤ6aに送信フォーム「16」によりその照合結果を送信する。プレーヤ6aではこの空き容量を記憶部に記憶する。送信がない場合には前述の処理を再度実行し、それでも送信がない場合にはプレイ処理を中止する。

【0068】次に、プレーヤ6aからプレーヤ6bに所定の送信フォーム「17」の内蔵コンテンツ販売IDの送信要求を行う。プレーヤ6bにおける記憶部6b-5内に内蔵コンテンツ販売IDが記録されている場合には、全コンテンツ販売IDをホスト認証に使用した認証AデータD2を鍵として16バイトづつDES暗号化し、このデータを所定の送信フォーム「18」によりプレーヤ6aに送信する。内蔵コンテンツ販売IDが無い場合にはその旨を所定の送信フォーム「18」により送信する。

【0069】次いで、プレーヤ6aがプレーヤ6bに対して所定の送信フォーム「19」、「20」、「21」でそれぞれ販売ヘッダ、販売サブヘッダ、コンテンツデータを順次を送信すると、プレーヤ6bがこれらに回答してプレーヤ6aに対して所定の送信フォーム「22」の各データ受信通知を送信する。次いで、プレーヤ6aでは、記憶部6b-5における転送販売ヘッダ再生鍵保存領域の2次暗号化再生鍵データを、暗号化／復号化部6a-6において自己プレーヤ(6a)のIDを鍵としてDES復号化し、1次暗号化再生鍵データを復号する。そして、この1次暗号化再生鍵データを、転送先であるプ

レーヤ6bのIDを鍵として再び2次DES暗号化処理を行い、この2次暗号化された再生鍵データを所定の送信フォーム[25]でプレーヤ6bに送信する。プレーヤ6bでは、この2次暗号化鍵データを記憶部6b-5の販売ヘッダの鍵データ保存領域に格納する。そして、電子財布部6b-2により販売チケット数分減額し、受信コンテンツの転送履歴を記憶部6mに記録する。そして、これらの処理が終了すると、所定の送信フォーム「26」の再生鍵データ受信通知をキオスク端末5に送信し、キオスク端末5とプレーヤ6aの間のIEEE1394インタフェースを切断する。

【0070】尚、前述の説明において、決裁ボックス7とプレーヤ6a、6b間のデータ転送手順を詳述しなかったが、図11で示したキオスク・プレーヤ間データ転送手順における[コンテンツ転送]及び[編集データ転送]の選択のステップを除き所定の送信フォーム[1]～[12]までの処理がほぼ同じで、その後処理として例えば前述の電子チケットが発行されるようになっている。従って、互いの機器の認証方式やプレーヤIDを送信する際の暗号化方式も同様である。

【0071】また、前述の鍵データは、プレーヤIDで暗号化し、復号化するようにしているが、例えば、プレーヤ6a、b内のコンテンツデータを記録する記憶部6a-5、6b-5が着脱自在のメモリデバイスのような記録媒体であるような場合には、記録媒体にIDを付与して、このIDに基づいて暗号化・復号化するようにしても良い。また、このように記憶部6b-5が着脱自在なような場合には、コンテンツデータを前記のように再生鍵でXOR演算で暗号化したまま状態で所定領域に記録すると共に、ヘッダ情報を暗号化したままの所定領域に記録するようにしても良い。

【0072】更に、前述の編集処理は、販売元端末であるキオスク端末及びPCCクライアントにおいてしか行えないようにしているが、それらに限らずコンテンツデータの改竄が行われないように暗号化されたままのデータを編集する等、著作権管理が工夫された編集装置なら良い。

【0073】また、更に、図30はテキストデータのフォーマットを示した図で、テキストデータは図30

(a)に示すように複数のテキスト「1」～「N」により構成され、テキスト「1」～「N」の各々は、図30(b)に示すように複数のテキストフレーム「1」～「N」により構成されている。テキストフレーム「1」～「N」の各々はともに、オーサリング時にコンテンツデータを暗号化したときと同じ暗号化方式で、再生鍵データと同じ16バイトで構成されて、3バイトのタイムスタンプと、1バイトのフレーム数と12バイトのテキストデータにより構成されている。そして、上記の暗号化、復号は、再生鍵データとテキストフレーム「1」～「N」ずつ、すなわち16バイトずつに排他的論理和

(XOR) 演算することにより行われている。

【0074】

【発明の効果】以上説明したように本発明によれば、コピーが行われないような暗号化を行うと共に、より速い再生速度での再生が要求される例えば実データであるコンテンツデータと、それほど速い処理速度での再生が要求されない例えばヘッダ情報等との暗号化方式を異ならせ、コンテンツデータの方は時間を要せずに復号化できる暗号化方式とし、ヘッダ情報の方は復号化に多少時間を要しても暗号がもれないような複雑な暗号化方式とすることで、再生鍵データが含まれる情報部を今まで以上に知られにくくすると共に、再生タイミングに支障をきたすようなことがないようにする。

【図面の簡単な説明】

【図1】本発明が採用されるキオスク端末を経由するコンテンツ販売システムの一例を示す構成図である。

【図2】本発明が採用されるインターネット形式によるコンテンツ販売システムの例を示す構成図である。

【図3】図1のプレーヤに配信される販売ヘッダの構成を示す説明図である。

【図4】図1のオーサリングにより付与される販売ヘッダの構成を示す説明図である。

【図5】図1のプレーヤに配信される販売サブヘッダの構成を示す説明図である。

【図6】図4及び図5内の転送制御データの構成を示す説明図である。

【図7】図1、図7のオーサリングシステムの1次暗号化処理を示すフローチャートである。

【図8】図1、図7のキオスク端末及びWebサーバの2次暗号化処理を示すフローチャートである。

【図9】図1、図7のコピー元プレーヤのコピー管理処理と2次暗号化処理を示すフローチャートである。

【図10】プレーヤの構成概略構成図である。

【図11】キオスク・プレーヤ間のデータ転送の手順を示す説明図である。

【図12】図11の連続した手順を示す説明図である。

【図13】転送フォームの構成図である。

【図14】発信元のコードの例を示す図である。

【図15】コマンドを示す図である。

【図16】図15以外のコマンドを示す図である。

【図17】図11において、編集データの転送が選択されたときの処理を示す説明図である。

【図18】インターネットサーバ・インターネットクライアント・プレーヤ間のデータ転送手順を示す説明図である。

【図19】図18に連続する説明図である。

【図20】図19に連続する説明図である。

【図21】図20に連続する説明図である。

【図22】図18においてコンテンツ編集・削除が選択されたときの手順を示す説明図である。

【図23】クライアントの編集処理を説明するための図である。

【図24】別のコンテンツ選択・購入の他の例で、図19～図21に対応する図である。

【図25】図24に連続する図である。

【図26】図25に連続する図である。

【図27】プレーヤ・プレーヤ間の転送手順を示す説明図である。

【図28】プレーヤ・プレーヤ間の他の例の転送手順を示す説明図である。

【図29】図28に連続する図である。

【図30】テキストデータのフォーマットを示す説明図である。

【符号の説明】

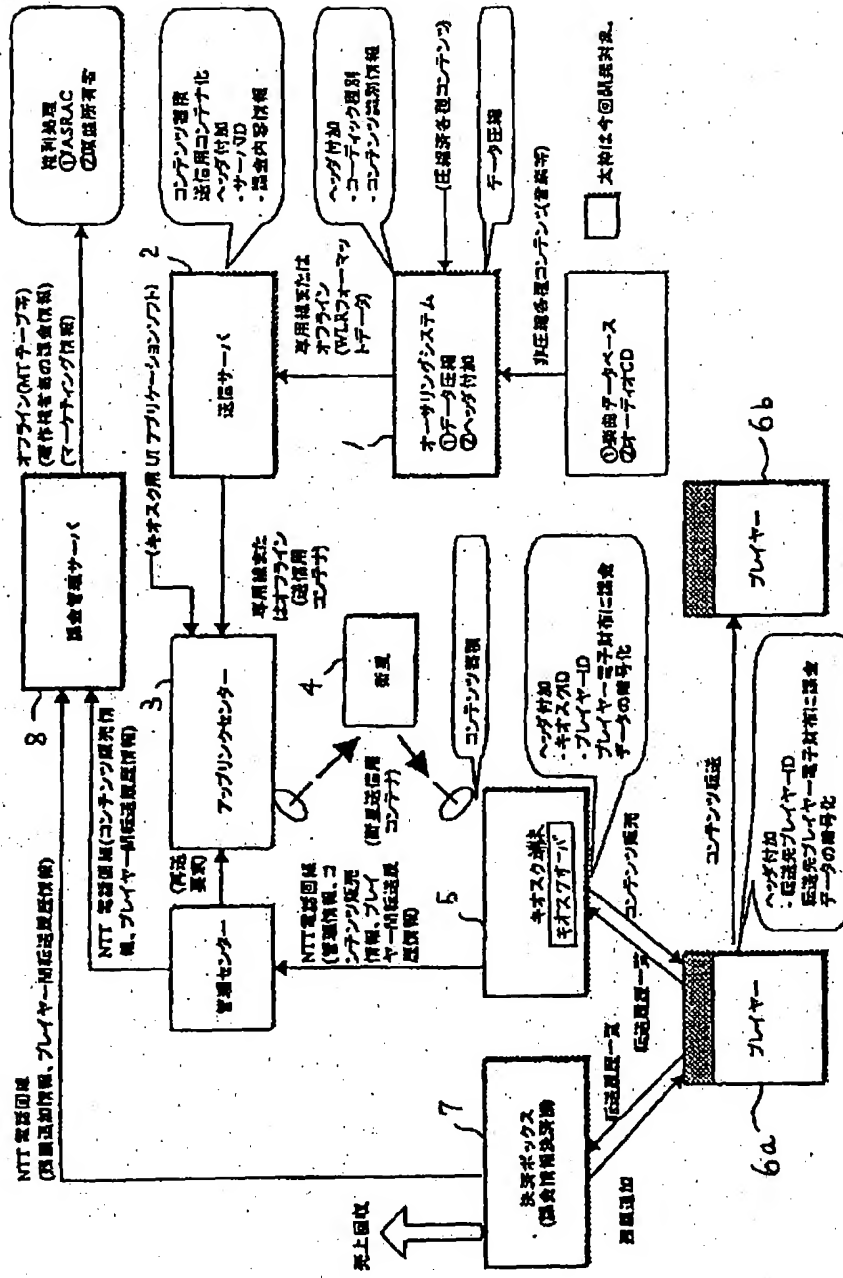
- 1 オーサリングシステム (ホスト)
- 2 送信サーバ
- 3 アップリンクセンタ
- 4 衛星
- 5 キオスク端末 (転送元端末、販売元端末)
- 6 a, 6 b プレーヤ (転送先端末、販売先端末)
- 6 a-1, 6 b-1 データインター転送フェース
- 6 a-2, 6 b-2 電子財布
- 6 a-3, 6 b-3 表示部
- 6 a-4, 6 b-4 操作部
- 6 a-5, 6 b-5, m 記憶部
- 6 a-6, 6 b-6 暗号化/復号化部
- 6 a-7, 6 b-7 データ圧縮/伸長部
- 6 a-8, 6 b-8 再生部
- 6 a-9, 6 b-9 出力端子
- 6 a-10, 6 b-10 制御部
- 9 Webサーバ (インターネットサーバ) (転送元端末)
- 10 インターネットサービス用PCクライアント

【図13】

転送フォームの一般形

発信元	コード	データ長(Byte)	データ
1 Byte	1 Byte	4 Bytes	

【図1】



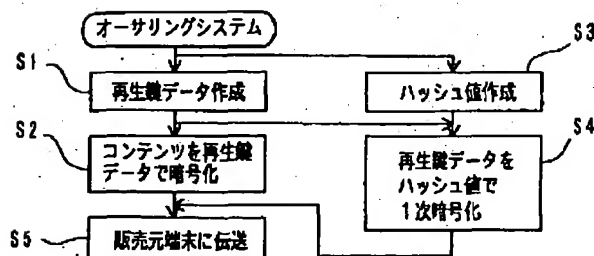
【図3】

販売ヘッダの構成

	b7	b0	b7	b0	b7	b0	b7	b0
0	販売ヘッダバージョン		販売ヘッダサイズ		Reserved (00h)		転送制御データ	
4	コンテンツ販売ID							
8								
12	転送元ID							
16								
20	販売チケット数				販売ヘッダ数		コンテンツ曲数	
24	JANPOSコード (52 bits) + "0" 12bits							
28								
32 ~ 60	制作タイトル名 (32 Bytes)							
64 ~ 76	制作会社名 (16 Bytes)							
80	1曲目データ長 (4 Bytes)							
84	2曲目データ長 (4 Bytes)							
~~~~~								
N曲目データ長 (4 Bytes)								
~~~~~								
1曲目の曲名								
~~~~~								
2曲目の曲名								
~~~~~								
N曲目の曲名								
~~~~~								
1曲目のアーティスト名								
32N+108 ~ 32N+132	2曲目のアーティスト名							
~~~~~								
N曲目のアーティスト名								
~~~~~								
1曲目の演奏時間 (時、分、秒、フレーム各 1 Byte)								
2曲目の演奏時間 (時、分、秒、フレーム各 1 Byte)								
~~~~~								
N曲目の演奏時間 (時、分、秒、フレーム各 1 Byte)								
~~~~~								
64N+M-K	再生鍵データ保存領域 (K Bytes)							

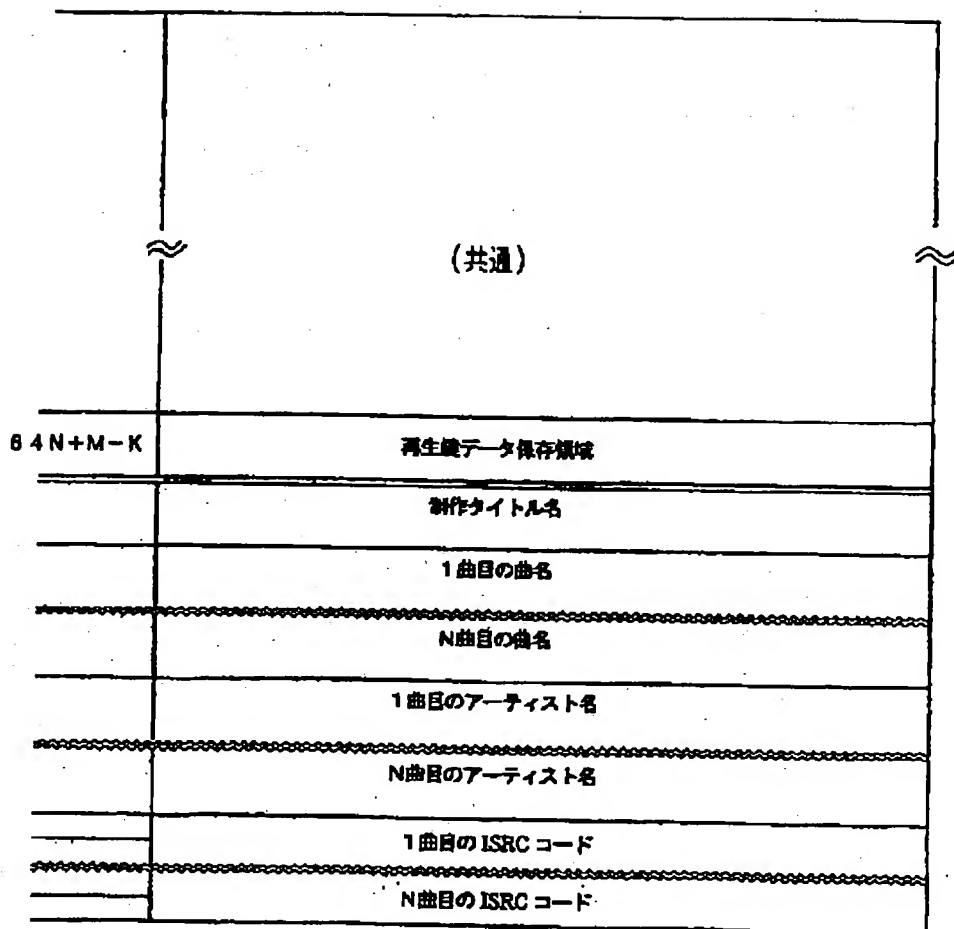
* 販売ヘッダ各項目の領域は全てマンドトリーとして割り当てられる。(領域を削除することは不可)  
データの無い領域は全て "0" で埋められる。

【図7】



【図4】

## マスタリング時の販売ヘッダ



【図6】

b0 ～ b3	再転送 世代数	0000: 再転送禁止 0001～1111: 再転送世代数(許可)
b4 ～ b7	再転送 禁止	0000: 再転送許可 0001: 再転送禁止 0010～1111: Reserved

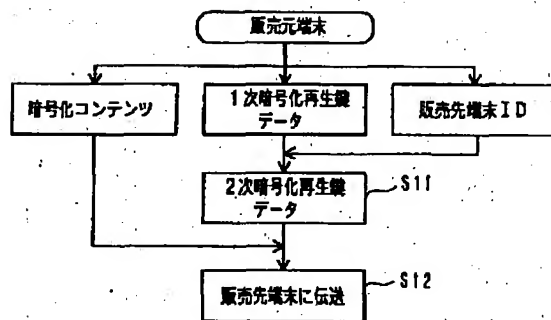
再転送世代数の制御法: 初期値に再転送許可世代数を設定。再転送時に1カウントダウンして上書き。  
0000にて再転送禁止

【図5】

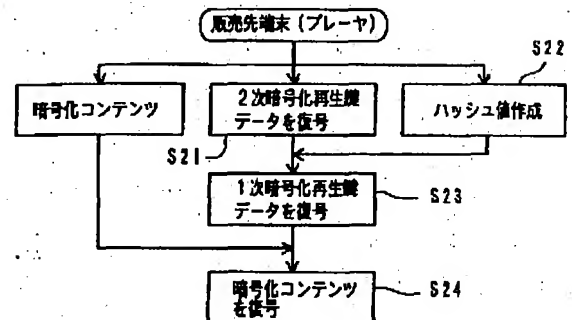
販売サブヘッダ (アルバム内の単曲販売用ヘッダ) の構成

	b7	b0	b7	b0	b7	b0	b7	b0
0	サブヘッダ バージョン		サブヘッダ サイズ		Reserved (00h)		転送制御データ	
4			コンテンツ販売 ID					
8								
12			転送元 ID					
16								
20	販売チケット数				00h		指定曲番 (1 Byte)	
24			JAN(POS)コード (52 bits) + "0" 12bits					
28								
32 ~ 60			制作タイトル名 (32 Bytes)					

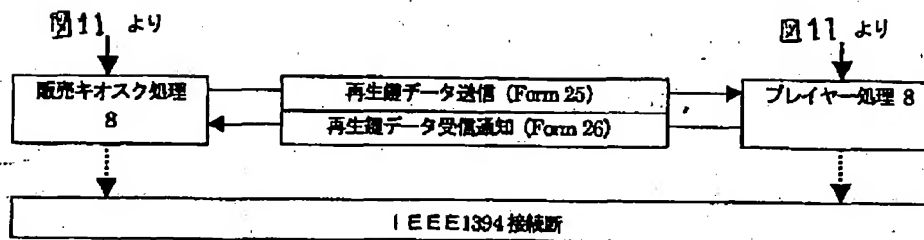
【図8】



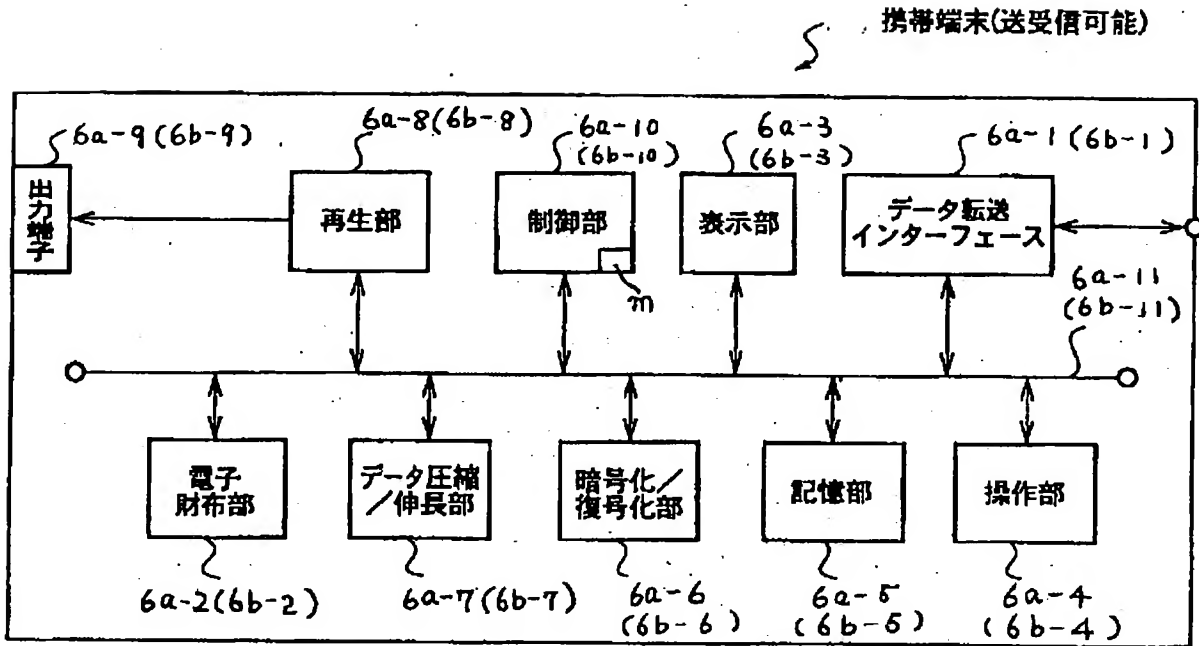
【図9】



【図12】



【図10】

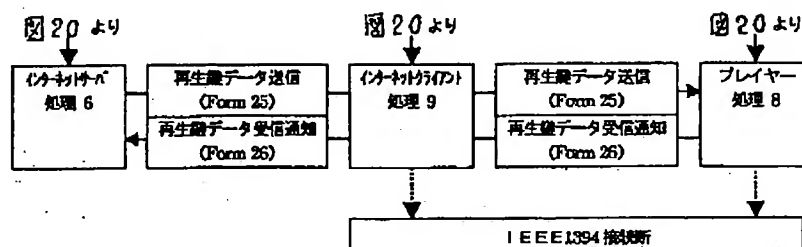


【図14】

システム構成装置(発信元)のコード

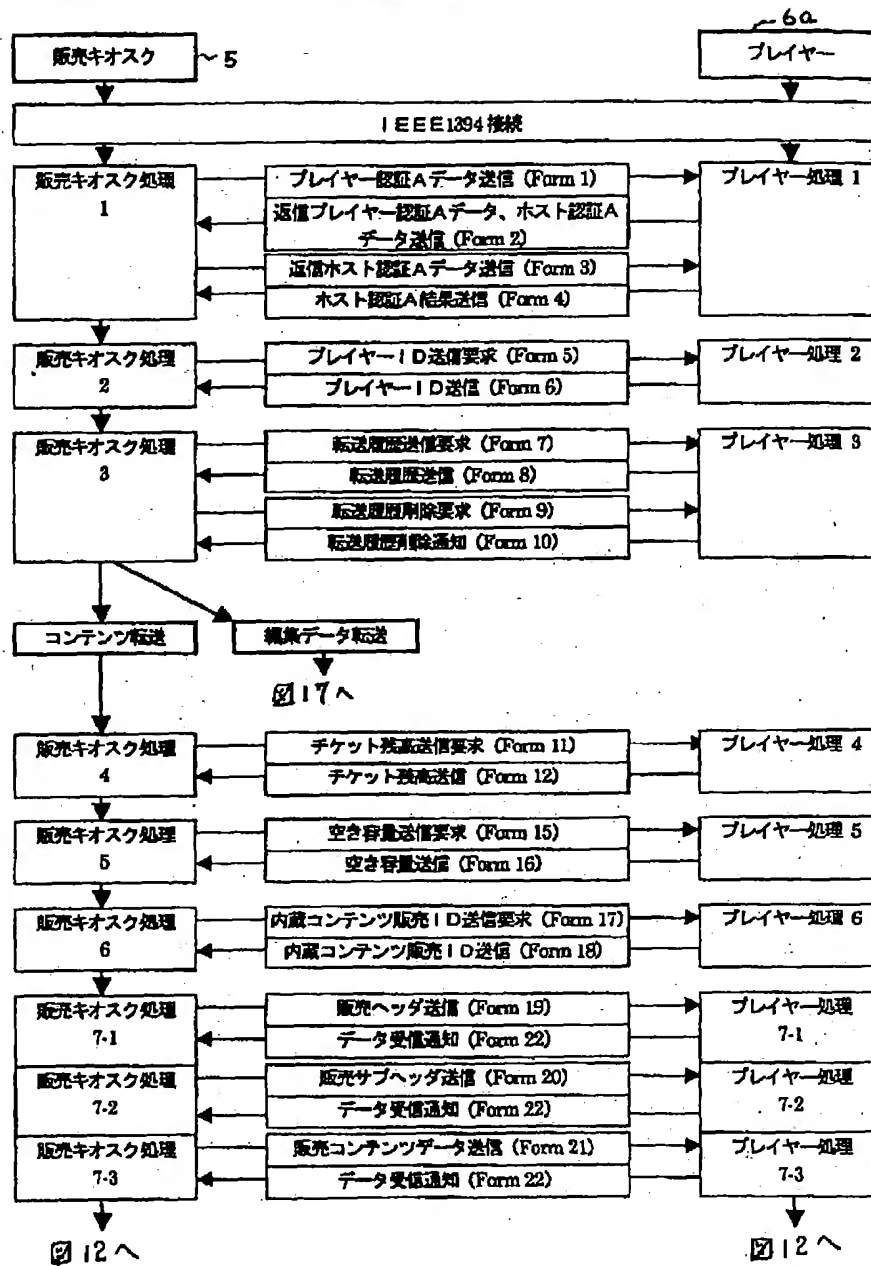
00h	Reserved	08h	Reserved
01h	プレイヤー	09h	チケットサーバ
02h	販売キオスク	0Ah	販売オスク運用管理サーバ
03h	決済ボックス	0Bh	課金管理サーバ
04h	インターネットコンテンツ管理部	0Ch	インターネットクライアント
05h	インターネット決済管理部	0Dh	送信サーバ
06h	Reserved	0Eh	マスタリング/オーサリング
07h	Reserved	0Fh~FFh	Reserved

【図21】



【図11】

販売キオスク・プレイヤー間データ転送基本手順



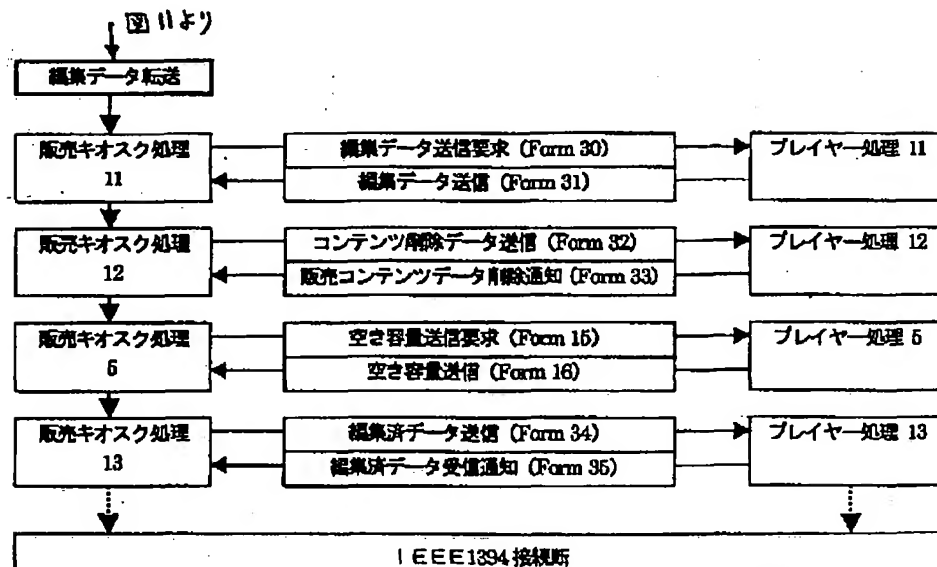


【図15】

## コマンド (1/2)

00h~0Fh	Reserved
10h	プレイヤー認証Aデータ送信
11h	返信ホスト認証Aデータ送信
12h	プレイヤーID送信要求
13h	転送履歴送信要求
14h	転送履歴削除要求
15h	チケット残高送信要求
16h	チケット発行終了通知
17h	Reserved
18h	Reserved
19h	空き容量送信要求
1Ah	内蔵コンテンツ販売ID送信要求
1Bh	販売ヘッダ送信
1Ch	販売サブヘッダ送信
1Dh	販売コンテンツデータ送信
1Eh	Reserved
1Fh	再生データ送信
20h	返信プレイヤー認証Aデータ、ホスト認証Aデータ送信
21h	ホスト認証A結果送信
22h	プレイヤーID送信
23h	転送履歴送信
24h	転送履歴削除通知
25h	チケット残高送信
26h	チケット発行受信通知
27h	Reserved
28h	Reserved
29h	空き容量送信
2Ah	内蔵コンテンツ販売ID送信

【図17】



【図16】

## コマンド(2/2)

2Bh	Reserved
2Ch	Reserved
2Dh	再生端データ受信通知
2Eh	プレイヤー認証Bデータ送信
2Fh	返信ホスト認証Bデータ送信
30h	編集データ送信要求
31h	コンテンツ削除データ送信
32h	編集済データ送信
33h	Reserved
34h	Reserved
35h	Reserved
36h	Reserved
37h	Reserved
38h	編集データ送信
39h	販売コンテンツデータ削除通知
3Ah	編集済データ受信通知
3Bh	Reserved
3Ch	Reserved
3Dh	Reserved
3Eh	返信プレイヤー認証Bデータ、ホスト認証Bデータ送信
3Fh	ホスト認証B結果送信
40h~EFh	Reserved
FBh	Reserved
F1h	データ受信通知
F2h	コマンド受信通知
F3h	コマンド再送信要求
F4h	待機コマンド送信
F5h	Reserved
F6h	Reserved
F7h	Reserved
F8h	Reserved
F9h	Reserved
FAh	電子チケット転送
FBh	Reserved
FCh	Reserved
FDh	Reserved
FEh	Reserved
FFh	中止コマンド送信

【図18】

インターネットサーバ・インターネットクライアント・プレイヤー間  
データ転送基本手順

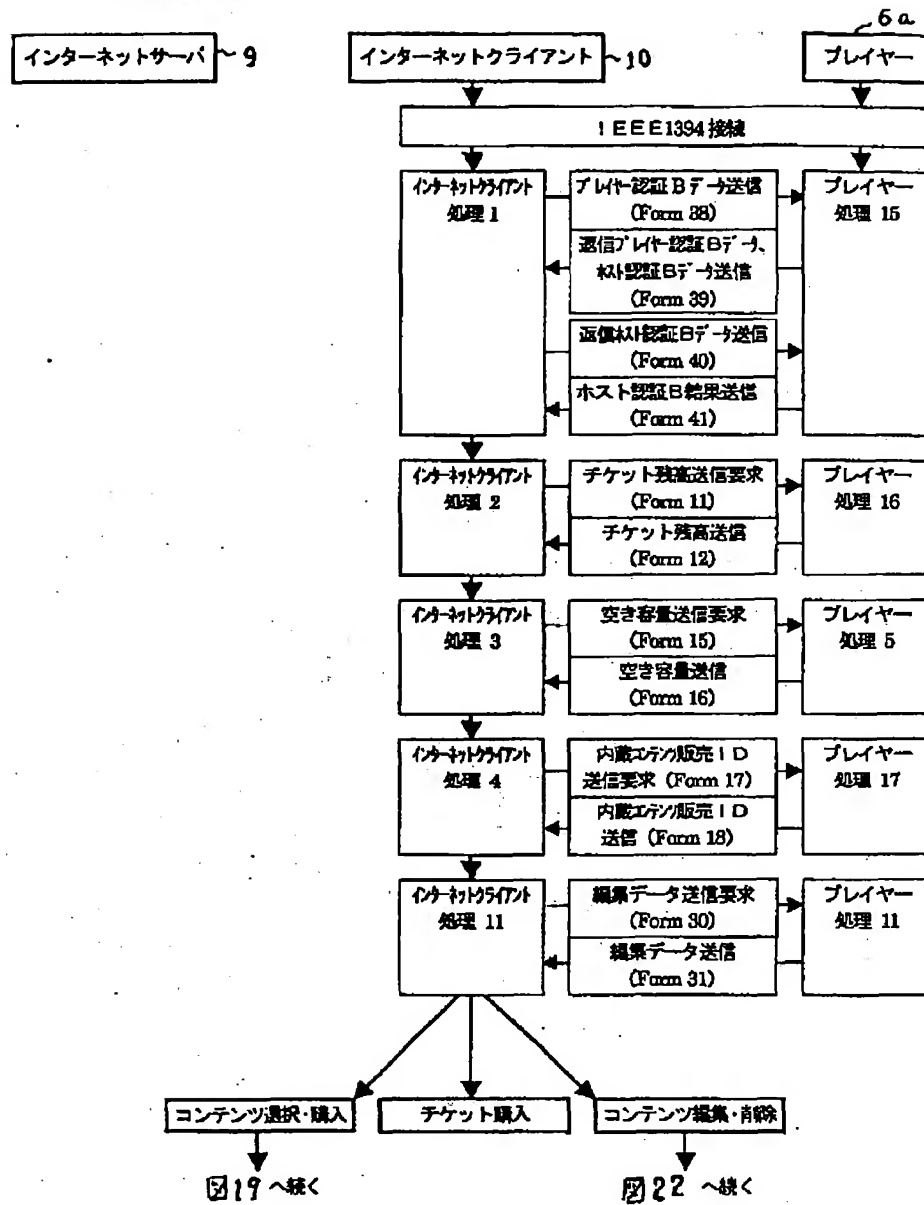


図18より

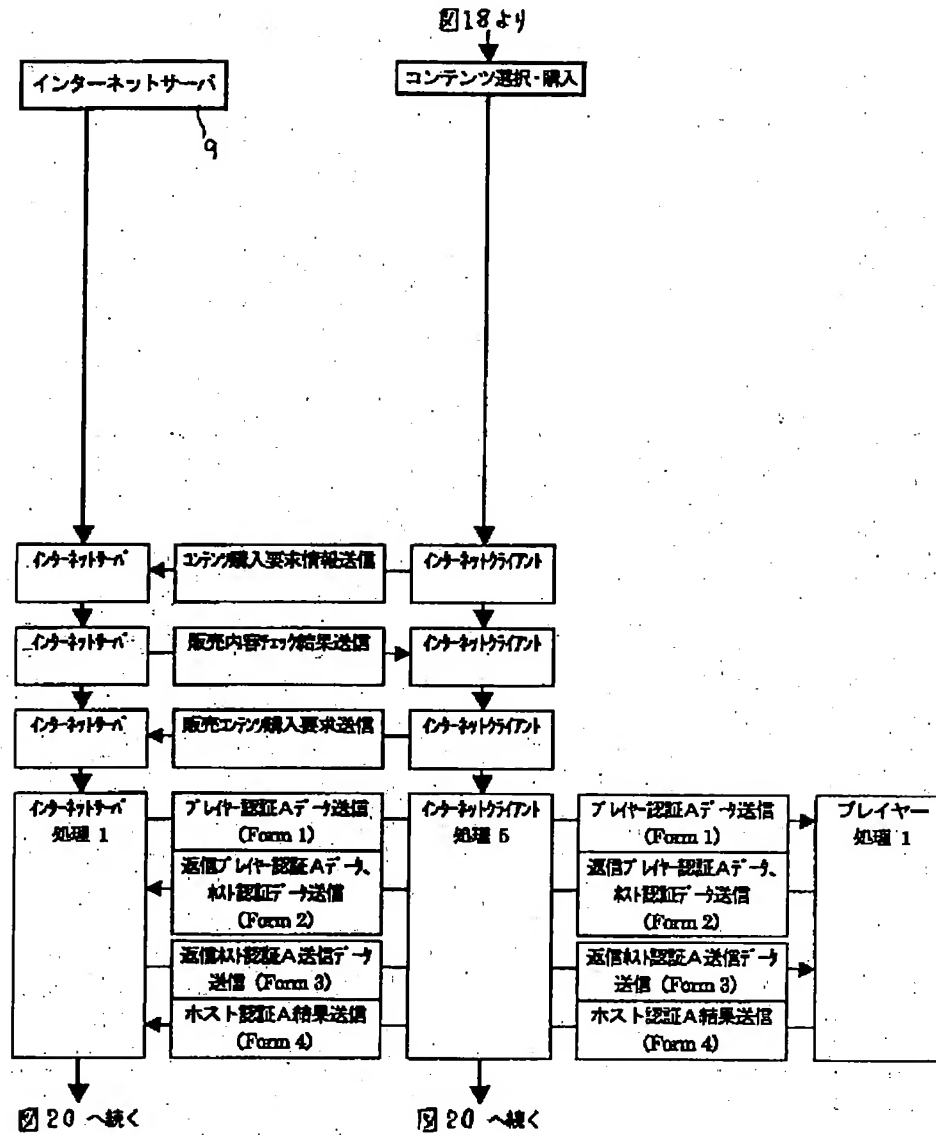


図28 より

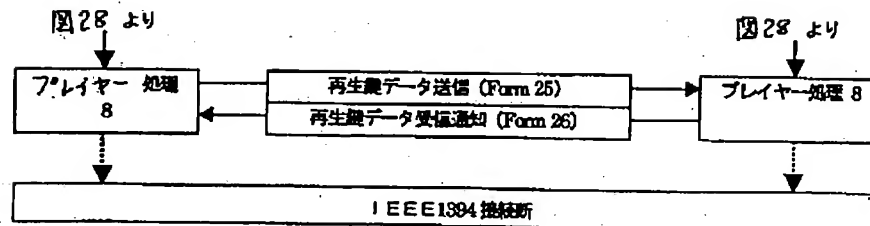
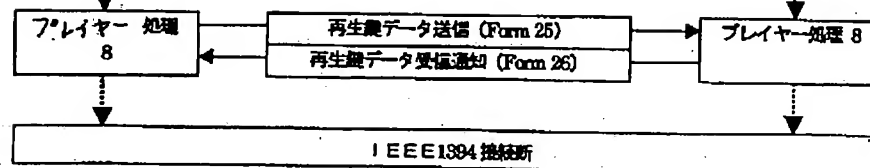
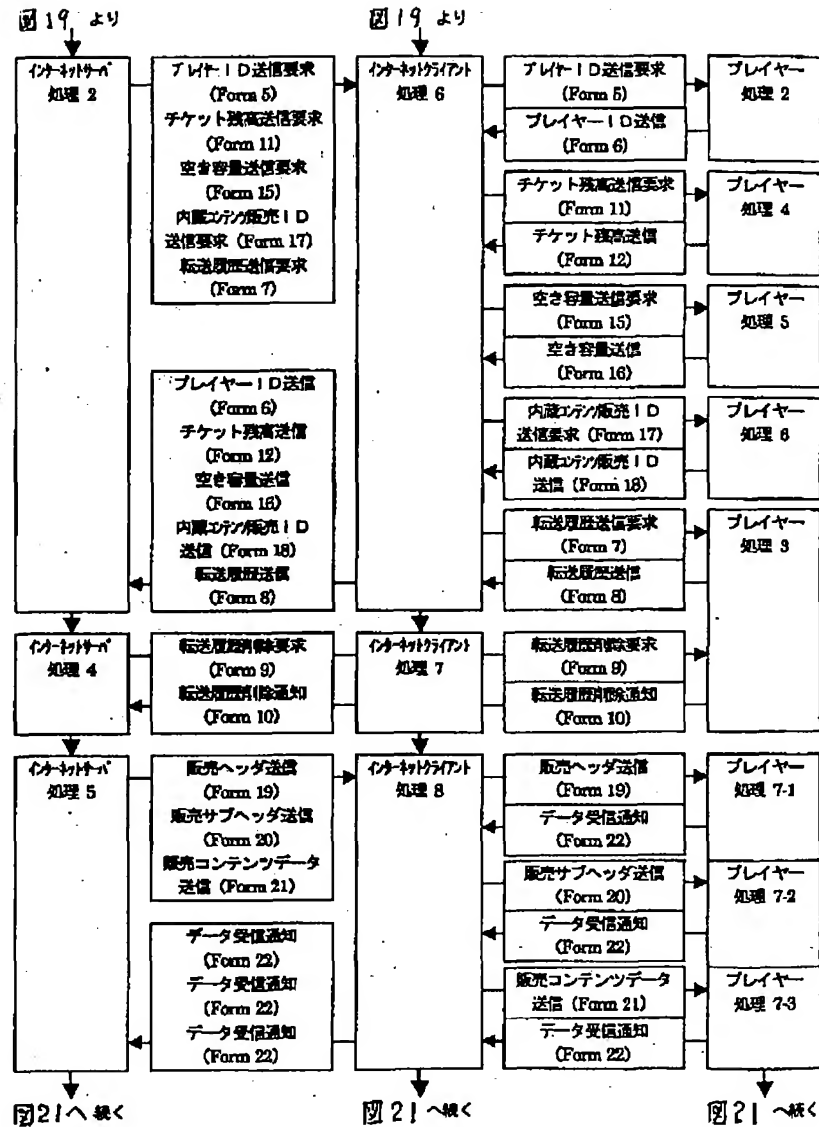


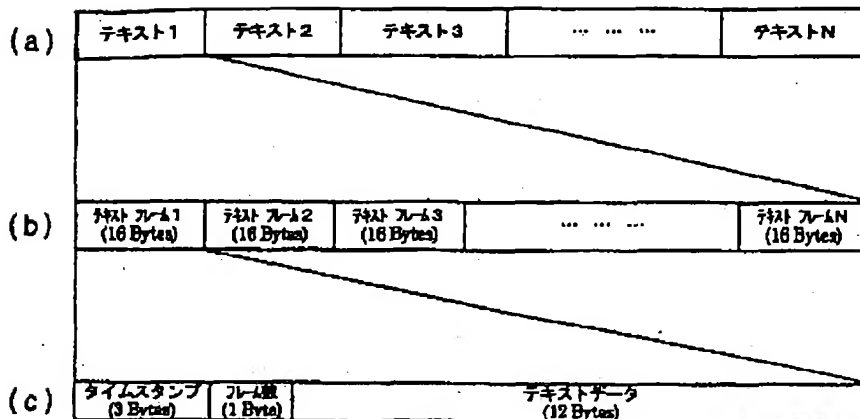
図28. より



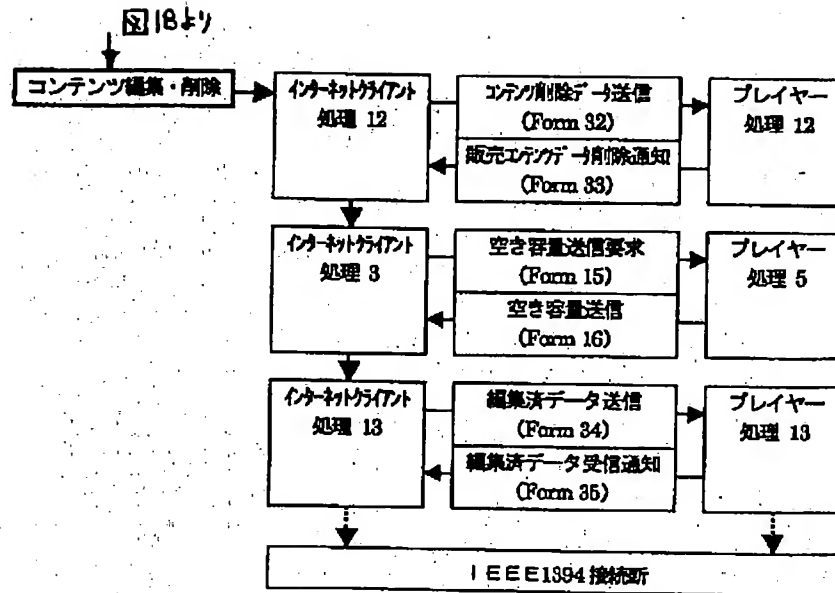
【図20】



【図30】



【図22】



【図23】

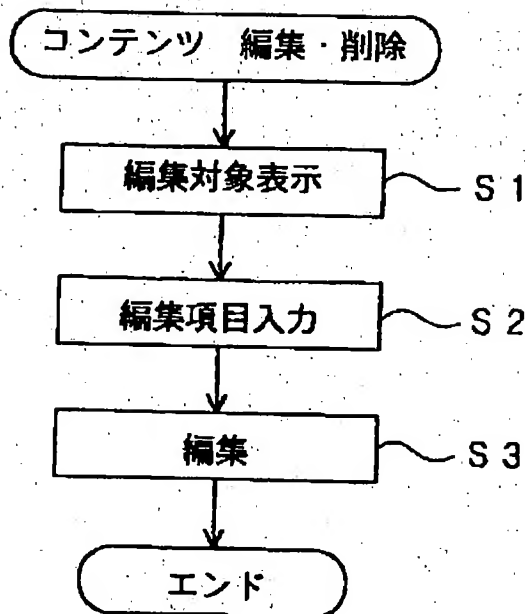
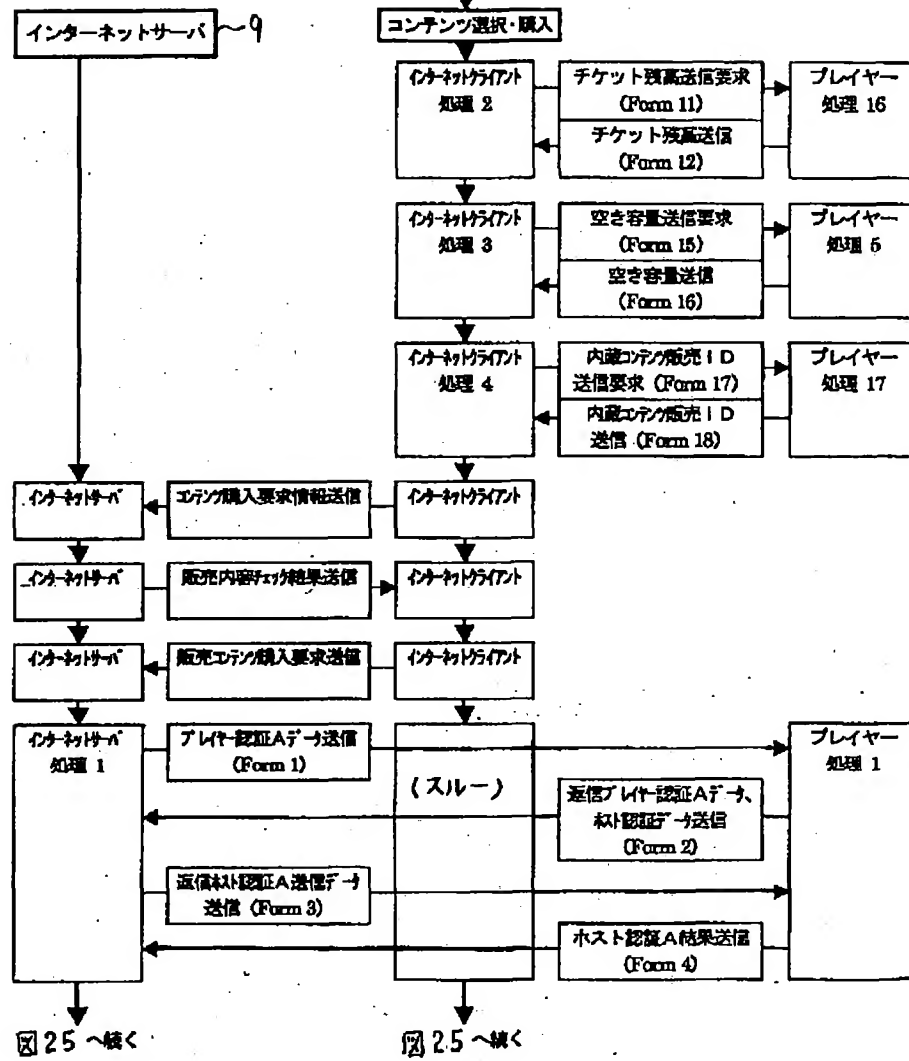
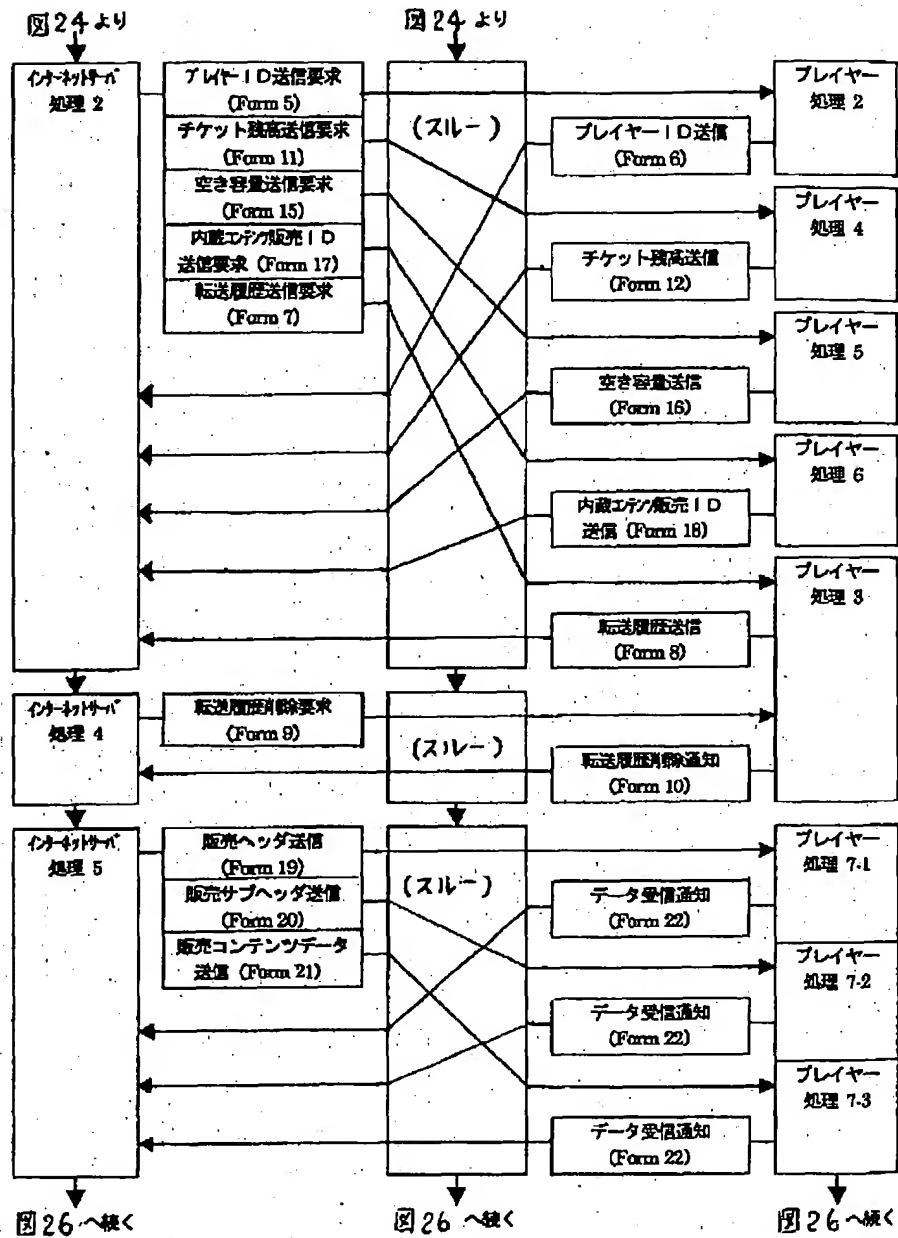




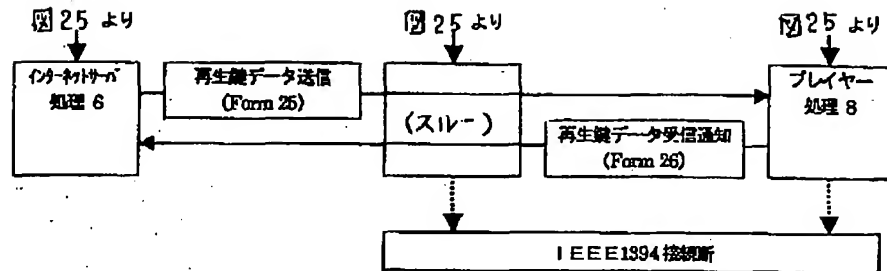
図 18 より



【図25】

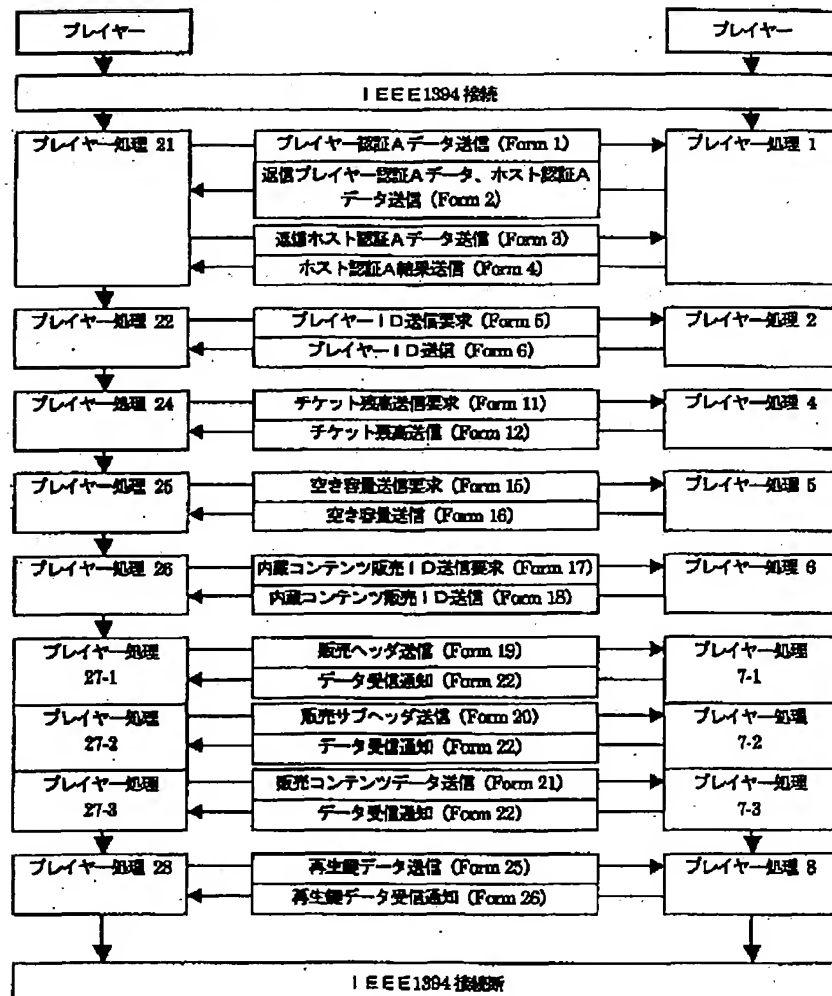


【図26】

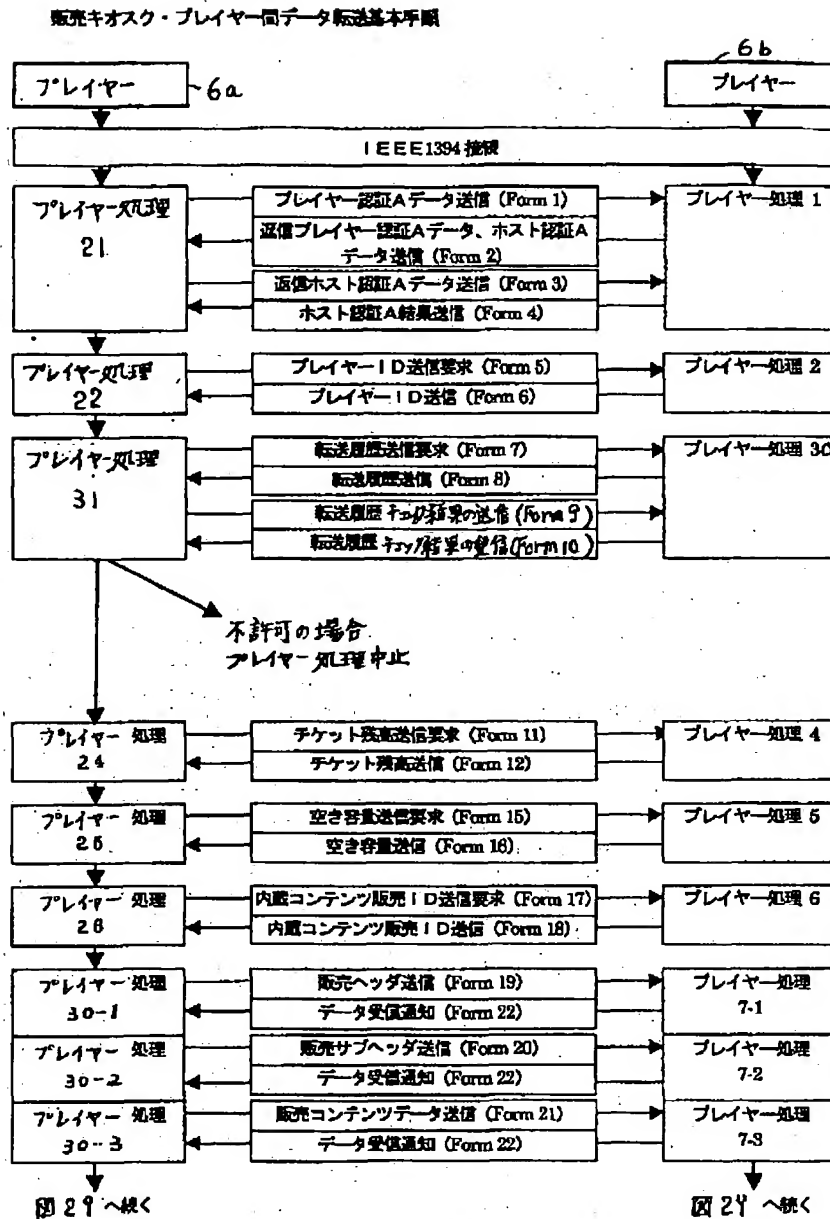


【図27】

## プレイヤー・プレイヤー間データ転送基本手順



【図28】



フロントページの続き

(51)Int.Cl.⁷

G10L 19/02  
19/00  
11/00

H04L 9/20  
H04N 7/167

識別記号

FI

G10L 7/04  
9/00

9/18  
H04L 9/00

キーワード(参考)

G 5J104

N

E

M

653

H O 4 N 7/167

Z

Fターム(参考) 5B017 AA06 BA05 BA07 BB03 BB10  
CA07 CA11 CA16  
5B082 AA11 CA07 CA08 EA01 EA12  
GA01 GA02 GC05  
5B085 AE06 AE13 AE29  
5C064 BA07 BB02 CA16 CB01 CC04  
5D045 DA20  
5J104 AA01 AA35 JA04 JA13 NA02  
PA07

